Object-image correspondence for curves under projections

Joseph M. Burdis*
North Carolina State University
joe.burdis@gmail.com

Irina A. Kogan †
North Carolina State University
iakogan@ncsu.edu
www.math.ncsu.edu/~iakogan

February 8, 2012

Abstract

We present a novel algorithm for deciding whether a given planar curve is an image of a given spatial curve, obtained by a central or a parallel projection with unknown parameters. A straightforward approach to this problem consists of setting up a system of conditions on the projection parameters and then checking whether or not this system has a solution. The main advantage of the algorithm presented here, in comparison to algorithms based on the straightforward approach, lies in a significant reduction of a number of real parameters that need to be eliminated in order to establish existence or non-existence of a projection that maps a given spatial curve to a given planar curve. Our algorithm is based on projection criteria that reduce the projection problem to a certain modification of the equivalence problem of planar curves under affine and projective transformations. The latter problem is then solved by differential signature construction based on Cartan's moving frame method. A similar approach can be used to decide whether a given finite set of ordered points on a plane is an image of a given finite set of ordered points in $\mathbb{R}^3$. The motivation comes from the problem of establishing a correspondence between an object and an image, taken by a camera with unknown position and parameters.

Keywords: Central and parallel projections, finite and affine cameras, curves, separating differential invariants, projective and affine transformations, geometric invariants, signatures, machine vision

*J. M. Burdis was partially supported by NSF grants CCF-0728801 and CCF-0347506.
†I. A. Kogan was partially supported by NSF grant CCF-0728801 and NSA grant H98230-11-1-0129.

Contents

1 Introduction

A central projection from $\mathbb{R}^3$ to $\mathbb{R}^2$ models a simple pinhole camera pictured in Figure 1 . A generic central projection is described by a linear fractional transformation (1):

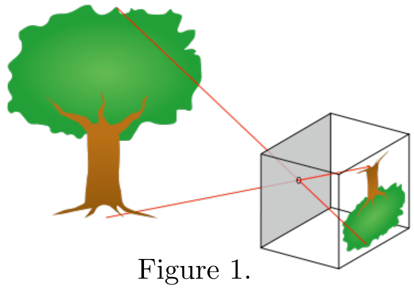

Figure 1.

$$\begin{aligned} x &= \frac{p_{11}\, z_1 + p_{12}\, z_2 + p_{13}\, z_3 + p_{14}}{p_{31}\, z_1 + p_{32}\, z_2 + p_{33}\, z_3 + p_{34}}, \\ y &= \frac{p_{21}\, z_1 + p_{22}\, z_2 + p_{23}\, z_3 + p_{24}}{p_{31}\, z_1 + p_{32}\, z_2 + p_{33}\, z_3 + p_{34}}, \end{aligned} \tag{1}$$

where (z_1, z_2, z_3) denote coordinates in $\mathbb{R}^3$,(x, y) denote coordinates in $\mathbb{R}^2$ and p_{ij}, $i = 1 \dots 3$, $j = 1 \dots 4$, are real parameters of the projection, such that the left 3×3 submatrix of 3×4 matrix $P = (p_{ij})$ has a non zero determinant. The parameters represent a freedom to choose the center of a projection, a position of image plane and, in general, non-orthogonal coordinate system on the image plane.[1] In the case when the distance between a camera and an object is significantly greater than the object depth a parallel projection provides a good camera model. A parallel projection has 8 parameters and can be described by a 3×4 matrix of rank 3, whose last row is $(0, 0, 0, 1)$. We review various camera models and related geometry in Section 2 (see also [14]). In most general terms, the projection problem considered here can be formulated as follows:

Problem 1. *Given a subset $\mathcal{Z}$ of $\mathbb{R}^3$ and a subset $\mathcal{X}$ of $\mathbb{R}^2$, does there exist a projection $P\colon \mathbb{R}^3 \to \mathbb{R}^2$ such that $\mathcal{X} = P(\mathcal{Z})$?*

A straightforward approach to this problem consists of setting up a system of conditions on the projection parameters and then checking whether or not this system has a solution. In the case when $\mathcal{Z}$ and $\mathcal{X}$ are finite lists of points, a solution based on the straightforward approach can be found in [14]. For curves and surfaces under central projections, this approach is taken in [9]. However, internal parameters of the camera are considered to be known in that paper and, therefore, there are only 6 in that study vs. 12 free parameters considered here. The method presented in [9] also uses an additional assumption that a planar curve $\mathcal{X} \subset \mathbb{R}^2$ has at least two points, whose tangent lines coincide. An alternative approach to the problem in the case when $\mathcal{Z}$ and $\mathcal{X}$ are *finite lists of points under parallel projections* was presented in [1, 2]. In these articles, the authors establish polynomial relationships that have to be satisfied by coordinates of the points in the sets $\mathcal{Z}$ and $\mathcal{X}$ in order for a projection to exists. Our approach to the projection problem for *curves* is closer in spirit to [1, 2], as we also establish necessary and sufficient conditions that curves $\mathcal{Z}$ and $\mathcal{X}$ must satisfy in order for a projection to exist. However, unlike [1, 2], we exploit the relationship between the projection problem and equivalence problem under group-actions. We will show below that, in comparison with the straightforward approach, our solution leads to a significant reduction of the number of parameters that have to be eliminated in order to solve Problem 1 for curves.

Throughout the paper, we assume that $\mathcal{Z}$ and $\mathcal{X}$ are algebraic curves and $\mathcal{Z}$ is not a straight line (and, therefore, its image under any projection is a one-dimensional constructible set). We will also relax the projection condition to $\mathcal{X} = \overline{P(\mathcal{Z})}$, *where bar throughout the paper denotes the algebraic*

[1] It is clear from (1) that multiplication of P by a non-zero constant does not change the projection map, therefore, we can identify P with a point of the projective space $\mathbb{PR}^{11}$, rather then a point in $\mathbb{R}^{12}$. However, since we do not know which of the parameters are non-zero, in computations we have to keep all 12 parameters.

closure of a set. In this section, as well as in Section 5, where algorithms and examples are presented, we make an additional assumption that $\mathcal{Z}$ and $\mathcal{X}$ have rational parameterization: $\mathcal{Z} = \{\Gamma(s)|s \in \mathbb{R}\}$ and $\mathcal{X} = \{\gamma(t)|t \in \mathbb{R}\}$, where $\Gamma\colon \mathbb{R} \to \mathbb{R}^3$ and $\gamma\colon \mathbb{R} \to \mathbb{R}^2$ are rational maps. This assumption is not essential. Algorithms for non-rational algebraic curves are placed in Appendix 8.5. Problem 1 for central projections of rational algebraic curves can be reformulated as the following real quantifier elimination problem:

Reformulation 1. (STRAIGHTFORWARD APPROACH) *Given rational maps $\Gamma\colon \mathbb{R} \to \mathbb{R}^3$ and $\gamma\colon \mathbb{R} \to \mathbb{R}^2$, determine the truth of the statement:*

$$\exists P \in \mathbb{R}^{3\times 4} \quad \det(p_{ij})_{i=1\ldots 3}^{j=1\ldots 3} \neq 0 \quad \forall s \in \mathbb{R} \quad \exists t \in \mathbb{R} \quad \gamma(t) = P(\Gamma(s)).$$

Real quantifier elimination problems are algorithmically solvable [22]. A survey of subsequent developments in this area can be found, for instance, in [16] and [6]. High computational complexity of these problems makes a reduction in the number of parameters to be desirable.

The projection criteria developed in this paper reduces the projection problem to the problem of deciding whether the given planar curve $\mathcal{X}$ is equivalent to a curve in a certain family of *planar* curves under an action of the projective group in the case of central projections, and under an action of the affine group in the case of parallel projections. The family of curves depends on 3 parameters in the case of central projections, and on 2 parameters in the case of parallel projections.

These group-equivalence problems can be solved by an adaptation of differential signature construction developed in [5] to solve *local* equivalence problems for smooth curves. In Section 4, we give an algebraic formulation of signature construction and show that it leads to a solution of *global* equivalence problems for algebraic curves. For this purpose we introduce a notion of *differentially separating set of invariants*. Following this method for the case of central projections, when $\mathcal{Z}$ and $\mathcal{X}$ are rational algebraic curves, we define two rational signature maps $\mathcal{S}_{\mathcal{X}}\colon \mathbb{R} \to \mathbb{R}^2$ and $\mathcal{S}_{\mathcal{Z}}\colon \mathbb{R}^4 \to \mathbb{R}^2$. Construction of these signature maps requires only differentiation and arithmetic operations and is computationally trivial. Problem 1 for central projections of rational algebraic curves becomes equivalent to:

Reformulation 2. (SIGNATURE APPROACH) *Given two rational maps $S_{\mathcal{X}}\colon \mathbb{R} \to \mathbb{R}^2$ and $S_{\mathcal{Z}}\colon \mathbb{R}^4 \to \mathbb{R}^2$, determine the truth of the statement:* $\exists c \in \mathbb{R}^3 \quad \forall s \in \mathbb{R} \quad \exists t \in \mathbb{R} \quad S_{\mathcal{Z}}(c, s) = S_{\mathcal{X}}(t)$.

We note that Reformulation 1 and Reformulation 2 have similar structure, but the former requires elimination of 14 parameters, while the latter requires elimination of only 5 parameters. (The case of parallel projection is treated in the similar manner and leads to the reduction of the number of real parameters that need to be eliminated from 10 to 4.)

Another advantage of the approach presented here is its universality: essentially the same method can be adapted to various types of the projections and various types of objects, both continuous and discrete. In Section 6, we discuss how this method leads to an alternative solution to the projection problem for finite lists of points (see [4] for more details). Our method can be also easily adapted to solve projection problems from $\mathbb{R}^n$ to a hyperplane. The problem and the solution remains valid if we replace $\mathbb{R}$ with $\mathbb{C}$, and in fact, as with most problems in algebraic geometry, the implementation of the algorithms is easier over the complex numbers (see also Remark 21 below). The existence of a complex projection provides a necessary but not a sufficient condition for the existence of a real projection.

Although the relation between projections and group actions is known, our literature search did not yield algorithms that exploit this relationship to solve the projection problem for curves in the generic setting of cameras with unknown internal and external parameters. The goal of

the paper is to introduce such algorithms. Although the development of efficient implementations of these algorithms and their complexity study lie outside of the scope of this paper, we made a preliminary implementations in MAPLE of projection algorithms over *complex numbers*. We implemented both an algorithm based on signature construction presented here and an algorithm based on the straightforward approach and timed their performance. The code and the experiments are posted at `www.math.ncsu.edu/~iakogan/symbolic/projections.html`.

In order to become practically useful in real-life applications, the algorithmic solution presented here, would have to be adapted to curves given by finite sampling of points. Some directions of such adaptation are indicated in Section 7 of the paper.

2 Projections and cameras

We will embed $\mathbb{R}^n$ into the projective space $\mathbb{PR}^n$ and use homogeneous coordinates on $\mathbb{PR}^n$ to express the map (1) by matrix multiplication.

Notation 1. Square brackets *around matrices (and, in particular, vectors) will be used to denote an equivalence class with respect to multiplication of a matrix by a nonzero scalar. Multiplication of equivalence classes of matrices A and B of appropriate sizes is well-defined by* $[A]\,[B] := [A\,B]$.

With this notation, a point $(x, y) \in \mathbb{R}^2$ corresponds to a point $[x, y, 1] = [\lambda x, \lambda y, \lambda] \in \mathbb{PR}^2$ for all $\lambda \neq 0$, and a point $(z_1, z_2, z_3) \in \mathbb{R}^3$ corresponds to $[z_1, z_2, z_3, 1] \in \mathbb{PR}^3$. We will refer to the points in $\mathbb{PR}^n$ whose last homogeneous coordinate is zero as *points at infinity*. In homogeneous coordinates projection (1) is a map $[P]\colon \mathbb{PR}^3 \to \mathbb{PR}^2$ given by

$$[x,\, y\,, 1]^{\mathrm{T}} = [P]\,[z_1,\, z_2,\, z_3,\, 1]^{\mathrm{T}}, \tag{2}$$

where P is 3×4 matrix of rank 3 and superscript T denotes transposition. Matrix P has a 1-dimensional kernel. Therefore, there exists a point $[z_1^0, z_2^0, z_3^0, z_4^0] \in \mathbb{PR}^3$ whose image under the projection is undefined (recall that $[0, 0, 0]$ is not a point in $\mathbb{PR}^2$). Geometrically, this point is the center of the projection.

In computer science literature (e.g. [14]), a camera is called *finite* if its center is not at infinity. A finite camera is modeled by a matrix P, whose left 3×3 submatrix is non-singular. Geometrically, finite cameras correspond to central projections from $\mathbb{R}^3$ to a plane. On the contrary, an *infinite* camera has its center at an infinite point of $\mathbb{PR}^3$. An infinite camera is modeled by a matrix P whose left 3×3 submatrix is singular. An infinite camera is called *affine* if the preimage of the line at infinity in $\mathbb{PR}^2$ is the plane at infinity in $\mathbb{PR}^3$. An affine camera is modeled by a matrix P whose last row is $(0, 0, 0, 1)$. In this case map (1) becomes $x = p_{11}\, z_1 + p_{12}\, z_2 + p_{13}\, z_3 + p_{14}\,, \quad y = p_{21}\, z_1 + p_{22}\, z_2 + p_{23}\, z_3 + p_{24}$. Geometrically, affine cameras correspond to *parallel projections* from $\mathbb{R}^3$ to a plane.[2] Eight degrees of freedom reflect a choice of the direction of a projection, a position of the image plane and a choice of linear system of coordinates on the image plane. An image plane may be assumed to be perpendicular to the direction of the projection, since other choices are absorbed in the freedom to choose, in general, non-orthogonal coordinate system on the image plane.

Definition 2. *The set of equivalence classes $[P]$, where $P = (p_{ij})_{j=1\ldots4}^{i=1\ldots3}$ is a 3×4 matrix whose left 3×3 submatrix is non-singular, is called* the set of central projections *and is denoted $\mathcal{CP}$.*

[2]Parallel projections are also called *generalized weak perspective projections* [1, 2].

The set of equivalence classes $[P]$*, where* $P = (p_{ij})_{j=1\ldots 4}^{i=1\ldots 3}$ *has rank 3 and its last row is* $(0,0,0,\lambda)$*,* $\lambda \neq 0$*, is called* the set of parallel projections *and is denoted* $\mathcal{PP}$*.*

Equation (1) determines a *central projection* when $[P] \in \mathcal{CP}$ and it determines a parallel projection when $[P] \in \mathcal{PP}$. Sets $\mathcal{CP}$ and $\mathcal{PP}$ are disjoint. Projections that are not included in these two classes correspond to infinite, non-affine cameras. These are not frequently used in computer vision and are not considered in this paper.

3 Projection criteria for curves

Recall that for every algebraic curve $\mathcal{X} \subset \mathbb{R}^n$ there exists a unique projective algebraic curve $[\mathcal{X}] \subset \mathbb{PR}^n$ such that $[\mathcal{X}]$ is the smallest projective variety containing $\mathcal{X}$ (see [11]).

Definition 3. *We say that a curve* $\mathcal{Z} \subset \mathbb{R}^3$ projects to $\mathcal{X} \subset \mathbb{R}^2$ *if there exists a* 3×4 *matrix* P *of rank 3 such that* $[\mathcal{X}] = \overline{\{[P][\mathbf{z}] \mid \mathbf{z} \in \mathcal{Z},\, P\mathbf{z} \neq 0\}}$*. We then write* $\mathcal{X} = P(\mathcal{Z})$ *or* $[\mathcal{X}] = [P][\mathcal{Z}]$*.*

Definition 4. *The* projective group $\mathcal{PGL}(n+1)$ *is a quotient of the general linear group* $\mathcal{GL}(n+1)$*, consisting of* $(n+1)\times(n+1)$ *non-singular matrices, by a 1-dimensional abelian subgroup* λI*, where* $\lambda \neq 0 \in \mathbb{R}$ *and* I *is the identity matrix. Elements of* $\mathcal{PGL}(n+1)$ *are equivalence classes* $[B] = [\lambda B]$*, where* $\lambda \neq 0$ *and* $B \in \mathcal{GL}(n+1)$*.*

The affine *group* $\mathcal{A}(n)$ *is a subgroup of* $\mathcal{PGL}(n+1)$ *whose elements* $[B]$ *have a representative* $B \in \mathcal{GL}(n+1)$ *with the last row equal to* $(0,\ldots,0,1)$*.*

The special affine *group* $\mathcal{SA}(n)$ *is a subgroup of* $\mathcal{A}(n)$ *whose elements* $[B]$ *have a representative* $B \in \mathcal{GL}(n+1)$ *with determinant* 1 *and the last row equal to* $(0,\ldots,0,1)$*.*

In homogeneous coordinates, the standard action of the projective group $\mathcal{PGL}(n+1)$ on $\mathbb{PR}^n$ is defined by multiplication:

$$[z_1,\ldots,z_n,z_0]^{\mathrm{T}} \to [B]\,[z_1,\ldots,z_n,z_0]^{\mathrm{T}}. \tag{3}$$

The action (3) induces linear-fractional action of $\mathcal{PGL}(n+1)$ on $\mathbb{R}^n$. In particular, for $n=2$, $[B] \in \mathcal{PGL}(3)$ we have

$$(x,y) \to \left(\frac{b_{11}\,x + b_{12}\,y + b_{13}}{b_{31}\,x + b_{32}\,y + b_{33}}, \quad \frac{b_{21}\,x + b_{22}\,y + b_{23}}{b_{31}\,x + b_{32}\,y + b_{33}}\right). \tag{4}$$

The restriction of (3) to $\mathcal{A}(n)$ induces an action on $\mathbb{R}^n$ consisting of compositions of linear transformations and translations. In particular, for $n=2$ and $[B] \in \mathcal{A}(2)$ represented by a matrix B whose last row is $(0,0,0,1)$

$$(x,y) \to (b_{11}\,x + b_{12}\,y + b_{13}, \quad b_{21}\,x + b_{22}\,y + b_{23})\,. \tag{5}$$

Definition 5. *We say that two curves* $\mathcal{X}_1 \subset \mathbb{R}^n$ *and* $\mathcal{X}_2 \subset \mathbb{R}^n$ *are* $\mathcal{PGL}(n+1)$*-equivalent if there exists* $[A] \in \mathcal{PGL}(n+1)$*, such that* $[\mathcal{X}_2] = \{[A][\mathbf{p}] \mid [\mathbf{p}] \in [\mathcal{X}_1]\}$*. We then write* $\mathcal{X}_2 = A(\mathcal{X}_1)$ *or* $[\mathcal{X}_2] = [A][\mathcal{X}_1]$*. If* $[A] \in G$*, where* G *is a subgroup of* $\mathcal{PGL}(n+1)$*, we say that* $\mathcal{X}_1$ *and* $\mathcal{X}_2$ *are* G*-equivalent.*

Before stating the projection criteria, we make the following simple, but important observations.

Proposition 6. *(i) If $\mathcal{Z} \subset \mathbb{R}^3$ projects to $\mathcal{X} \subset \mathbb{R}^2$ by a* parallel projection*, then any curve that is $\mathcal{A}(3)$-equivalent to $\mathcal{Z}$ projects to any curve that is $\mathcal{A}(2)$-equivalent to $\mathcal{X}$ by a* parallel projection*. In other words, parallel projections are defined on affine equivalence classes of curves.*

(ii) If $\mathcal{Z} \subset \mathbb{R}^3$ projects to $\mathcal{X} \subset \mathbb{R}^2$ by a central projection *then any curve in $\mathbb{R}^3$ that is $\mathcal{A}(3)$-equivalent to $\mathcal{Z}$ projects to any curve on $\mathbb{R}^2$ that is $\mathcal{PGL}(3)$-equivalent to $\mathcal{X}$ by a* central projection*.*

Proof. (i) Assume that there exists a parallel projection $[P] \in \mathcal{PP}$ such that $[\mathcal{X}] = [P][\mathcal{Z}]$. Then for all $(A, B) \in \mathcal{A}(2) \times \mathcal{A}(3)$ we have $[A]\,[\mathcal{X}] = [A]\,[P]\,[B^{-1}]\,[B]\,[\mathcal{Z}]$. Since $[A]\,[P]\,[B^{-1}] \in \mathcal{PP}$, curve $B(\mathcal{Z})$ projects to $A(\mathcal{X})$. (ii) is proved similarly. □

Remark 7. *It is known that if $\mathcal{X}_1$ and $\mathcal{X}_2$ are images of a curve $\mathcal{Z}$ under two central projections* with the same center*, then $\mathcal{X}_1$ and $\mathcal{X}_2$ are $\mathcal{PGL}(3)$-equivalent, but if the centers of the projections are not the same this is no longer true (see Example 28). Similarly, images of $\mathcal{Z}$ under different parallel projections may not be $\mathcal{A}(2)$-equivalent (see Example 31).*

Theorem 8. *(*CENTRAL PROJECTION CRITERIA*) A curve $\mathcal{Z} \subset \mathbb{R}^3$ projects to a curve $\mathcal{X} \subset \mathbb{R}^2$ by a* central projection *if and only if there exist $c_1, c_2, c_3 \in \mathbb{R}$ such that $\mathcal{X}$ is $\mathcal{PGL}(3)$-equivalent to*

$$\tilde{\mathcal{Z}}_{c_1,c_2,c_3} = \overline{\left\{ \left(\frac{z_1 + c_1}{z_3 + c_3}, \quad \frac{z_2 + c_2}{z_3 + c_3} \right) \,\middle|\, (z_1, z_2, z_3) \in \mathcal{Z} \right\}} \subset \mathbb{R}^2. \tag{6}$$

Proof. ($\Rightarrow$) Assume there exists a central projection $[P]$ such that $[\mathcal{X}] = [P]\,[\mathcal{Z}]$. Then P is a 3×4 matrix $P = (p_{ij})_{j=1\ldots4}^{i=1\ldots3}$ whose left 3×3 submatrix is non-singular. Therefore there exist $c_1, c_2, c_3 \in \mathbb{R}$ such that $p_{*4} = c_1\, p_{*1} + c_2\, p_{*2} + c_3\, p_{*3}$, where p_{*j} denotes the j-th column of the matrix P. We observe that

$$[A][P^0_{\mathcal{C}}][B] = [P]\,, \tag{7}$$

where $A := (p_{ij})_{j=1\ldots3}^{i=1\ldots3}$ is 3×3 submatrix of P,

$$P^0_{\mathcal{C}} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ and } B := \begin{pmatrix} 1 & 0 & 0 & c_1 \\ 0 & 1 & 0 & c_2 \\ 0 & 0 & 1 & c_3 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{8}$$

Note that $[A]$ belongs to $\mathcal{PGL}(3)$. Since

$$[P^0_{\mathcal{C}}][B][z_1, z_2, z_3,\, 1]^{\mathrm{T}} = [z_1 + c_1, z_2 + c_2, z_3 + c_3]^{\mathrm{T}},$$

then $[\mathcal{X}] = [A][\tilde{\mathcal{Z}}_{c_1,c_2,c_3}]$, where $\tilde{\mathcal{Z}}_{c_1,c_2,c_3}$ is defined by (6).

($\Leftarrow$) To prove the converse direction we assume that there exists $[A] \in \mathcal{PGL}(3)$ and $c_1, c_2, c_3 \in \mathbb{R}$ such that $[\mathcal{X}] = [A][\tilde{\mathcal{Z}}_{c_1,c_2,c_3}]$, where $[\tilde{\mathcal{Z}}_{c_1,c_2,c_3}]$ is defined by (6). A direct computation shows that $\mathcal{Z}$ is projected to $\mathcal{X}$ by the central projection $[P] = [A]\,[P^0_{\mathcal{C}}]\,[B]$, where B and $[P^0_{\mathcal{C}}]$ are given by (8). □

Theorem 9. *(*PARALLEL PROJECTION CRITERIA.*) A curve $\mathcal{Z} \subset \mathbb{R}^3$ projects to a curve $\mathcal{X} \subset \mathbb{R}^2$ by an parallel projection if and only if there exist $c_1, c_2 \in \mathbb{R}$ and an ordered triplet $(i, j, k) \in \{(1, 2, 3),\, (1, 3, 2),\, (2, 3, 1)\}$ such that $\mathcal{X}$ is $\mathcal{A}(2)$-equivalent to*

$$\tilde{\mathcal{Z}}^{i,j,k}_{c_1,c_2} = \overline{\left\{ (z_i + c_1\, z_k, \quad z_j + c_2\, z_k) \,\middle|\, (z_1, z_2, z_3) \in \mathcal{Z} \right\}} \subset \mathbb{R}^2. \tag{9}$$

Proof. ($\Rightarrow$)Assume there exists a parallel projection $[P]$ such that $[\mathcal{X}] = [P]\,[\mathcal{Z}]$. Then $[P]$ can be represented by a matrix:

$$P = \begin{pmatrix} p_{11} & p_{12} & p_{13} & p_{14} \\ p_{21} & p_{22} & p_{23} & p_{24} \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{10}$$

of rank 3. Therefore there exist $1 \leq i < j \leq 3$ such that the rank of the submatrix $\begin{pmatrix} p_{1i} & p_{1j} \\ p_{2i} & p_{2j} \end{pmatrix}$ is 2. Then for $1 \leq k \leq 3$, such that $k \neq i$ and $k \neq j$, there exist $c_1,\, c_2 \in \mathbb{R}$, such that $\begin{pmatrix} p_{1k} \\ p_{2k} \end{pmatrix} = c_1 \begin{pmatrix} p_{1i} \\ p_{2i} \end{pmatrix} + c_2 \begin{pmatrix} p_{1j} \\ p_{2j} \end{pmatrix}$. We define $A := \begin{pmatrix} p_{1i} & p_{1j} & p_{14} \\ p_{2i} & p_{2j} & p_{24} \\ 0 & 0 & 1 \end{pmatrix}$ and define B to be the matrix whose columns are vectors $b_{*i} := (1,0,0,0)^{\mathrm{T}}$, $b_{*j} := (0,1,0,0)^{\mathrm{T}}$, $b_{*k} := (c_1, c_2, 1, 0)^{\mathrm{T}}$, $b_{*4} = (0,0,0,1)^{\mathrm{T}}$. We observe that $[A][P^0_{\mathcal{P}}][B] = [P]$, where $P^0_{\mathcal{P}} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. Since $[P^0_{\mathcal{P}}][B][\mathcal{Z}] = [\tilde{\mathcal{Z}}^{i,j,k}_{c_1,c_2}]$, then $[\mathcal{X}] = [A][\tilde{\mathcal{Z}}^{i,j,k}_{c_1,c_2}]$. Observe that $[A] \in \mathcal{A}(2)$ and the direct statement is proved.

($\Leftarrow$) To prove the converse direction we assume that there exist $[A] \in \mathcal{A}(2)$, two real numbers c_1 and c_2, and a triplet of indices $(i,\, j,\, k) \in \{(1,2,3),\, (1,3,2),\, (2,3,1)\}$, such that $[\mathcal{X}] = [A][\tilde{\mathcal{Z}}^{i,j,k}_{c_1,c_2}]$, where the planar curve $\tilde{\mathcal{Z}}^{i,j,k}_{c_1,c_2}(s)$ is given by (9). Let $P^0_{\mathcal{P}}$ and B be a matrix defined in the first part of the proof. A direct computation shows that $\mathcal{Z}$ is projected to $\mathcal{X}$ by the parallel projection $[P] = [A][P^0_{\mathcal{P}}][B]$. $\square$

The families of curves $\tilde{\mathcal{Z}}^{i,j,k}_{c_1,c_2}$ given by (9) have a large overlap. The following corollary eliminates this redundancy and, therefore, is useful for practical computations.

Corollary 10. (REDUCED PARALLEL PROJECTION CRITERIA) *A curve $\mathcal{Z} \subset \mathbb{R}^3$ projects to $\mathcal{X} \subset \mathbb{R}^2$ by a parallel projection if and only if there exist $a_1, a_2, b \in \mathbb{R}$ such that the curve $\mathcal{X}$ is $\mathcal{A}(2)$-equivalent to one of the following* planar *curves:*

$$\tilde{\mathcal{Z}}_{a_1,a_2} = \overline{\left\{(z_1 + a_1\, z_3,\, z_2 + a_2\, z_3)\,\middle|\,(z_1,z_2,z_3) \in \mathcal{Z}\right\}} \subset \mathbb{R}^2, \tag{11}$$

$$\tilde{\mathcal{Z}}_{b} = \overline{\left\{(z_1 + b\, z_2,\, z_3)\,\middle|\,(z_1,z_2,z_3) \in \mathcal{Z}\right\}} \subset \mathbb{R}^2, \tag{12}$$

$$\tilde{\mathcal{Z}} = \overline{\left\{(z_2,\, z_3)\,\middle|\,(z_1,z_2,z_3) \in \mathcal{Z}\right\}} \subset \mathbb{R}^2. \tag{13}$$

Proof. We first prove that for any permutation (i,j,k) of numbers $(1,2,3)$, such that $i < j$, and for any $c_1, c_2 \in \mathbb{R}$ the set $\tilde{\mathcal{Z}}^{i,j,k}_{c_1,c_2} = \left\{(z_i + c_1\, z_k,\, z_j + c_2\, z_k)\,\middle|\,(z_1,z_2,z_3) \in \mathcal{Z}\right\}$ is $\mathcal{A}(2)$-equivalent to one of the sets listed in (11) – (13).

Obviously, $\tilde{\mathcal{Z}}^{1,2,3}_{c_1,c_2} = \tilde{\mathcal{Z}}_{a_1,a_2}$ with $a_1 = c_1$ and $a_2 = c_2$.

For $\tilde{\mathcal{Z}}^{1,3,2}_{c_1,c_2}$, if $c_2 \neq 0$ then $\begin{pmatrix} 1 & -\frac{c_1}{c_2} \\ 0 & \frac{1}{c_2} \end{pmatrix} \begin{pmatrix} z_1 + c_1 z_2 \\ z_3 + c_2 z_2 \end{pmatrix} = \begin{pmatrix} z_1 - \frac{c_1}{c_2} z_3 \\ z_2 + \frac{1}{c_2} z_3 \end{pmatrix}$ and so $\tilde{\mathcal{Z}}^{1,3,2}_{c_1,c_2}$ is $\mathcal{A}(2)$-equivalent to $\tilde{\mathcal{Z}}_{a_1,a_2}$ with $a_1 = -\frac{c_1}{c_2}$ and $a_2 = \frac{1}{c_2}$. Otherwise, if $c_2 = 0$, the $\tilde{\mathcal{Z}}^{1,3,2}_{c_1,c_2} = \tilde{\mathcal{Z}}_b$ with $b = c_1$.

Similarly for $\tilde{\mathcal{Z}}^{2,3,1}_{c_1,c_2}$, if $c_2 \neq 0$ then $\tilde{\mathcal{Z}}^{2,3,1}_{c_1,c_2}$ is $\mathcal{A}(2)$-equivalent to $\tilde{\mathcal{Z}}_{a_1,a_2}$ with $a_1 = \frac{1}{c_2}$ and $a_2 = -\frac{c_1}{c_2}$. Otherwise, if $c_2 = 0$, then $\tilde{\mathcal{Z}}^{2,3,1}_{c_1,c_2} = (z_2 + c_1 z_1,\, z_3)$. If $c_1 \neq 0$ then $\tilde{\mathcal{Z}}^{2,3,1}_{c_1,c_2}$ is $\mathcal{A}(2)$-equivalent to $\tilde{\tilde{\mathcal{Z}}}_b$ with $b = \frac{1}{c_1}$, otherwise $c_1 = 0$ and $\tilde{\mathcal{Z}}^{2,3,1}_{c_1,c_2} = \tilde{\tilde{\mathcal{Z}}}$.

We can reverse the argument and show that any curve given by (11)–(13) is $\mathcal{A}(2)$-equivalent to a curve from family (9). Then the reduced criteria follows from Theorem 9. $\square$

4 Group-equivalence problem

Theorems 8 and 9 reduce the projection problem to the problem of establishing group-action equivalence between a given curve and a curve from a certain family. A variety of methods exist to solve group-equivalence problem for curves. We base our algorithm on the differential signature construction described in [5]. The differential signature proposed there solves the *local* equivalence problem for smooth curves. We adapt this construction to the algebraic setting and prove that the differential signature gives a solution of the *global* equivalence problem in the case of algebraic curves. For this purpose, we introduce a notion of a *differentially separating set of invariants.* We discuss the possibility of using some other methods for solving the equivalence problem in Section 7.

4.1 Differential invariants for planar curves

A rational action of an algebraic group G on $\mathbb{R}^2$ can be prolonged to an action on the n-th jet space $J^n = \mathbb{R}^{n+2}$ with coordinates $(x, y, y^{(1)}, \dots, y^{(n)})$ as follows.[3] For a fixed $g \in G$, let $(\bar{x}, \bar{y}) = g \cdot (x, y)$. Then $\bar{x}, \bar{y}$ are rational functions of (x, y) and

$$g \cdot (x, y, y^{(1)}, \dots, y^{(n)}) = (\bar{x}, \bar{y}, \bar{y}^{(1)}, \dots, \bar{y}^{(n)}), \text{ where} \tag{14}$$
$$\bar{y}^{(1)} = \frac{\frac{d}{dx}\left[\bar{y}(x,y)\right]}{\frac{d}{dx}\left[\bar{x}(x,y)\right]}, \dots, \bar{y}^{(k+1)} = \frac{\frac{d}{dx}\left[\bar{y}^{(k)}(x, y, y^{(1)}, \dots, y^{(k)})\right]}{\frac{d}{dx}\left[\bar{x}(x,y)\right]}, \quad k = 1, \dots, n-1.$$

In (14), $\frac{d}{dx}$ is the total derivative, applied under assumption that y is function of x.[4] We note that the natural projection $\pi^n_k \colon J^n \to J^k$, $k < n$ is equivariant with respect to action (14).

Definition 11. *A function on J^n is called* a differential function. *The* order of a differential function *is the maximum value of k such that the function explicitly depends on the variable $y^{(k)}$.*

A differential function which is invariant under action (14) is called a differential invariant.

Remark 12. *Due to equivariant property of the projection $\pi^n_k \colon J^n \to J^k$, $k < n$, a differential invariant of order k on J^k can be viewed as a differential invariant on J^n for all $n \geq k$.*

Definition 13. *Let G act on $\mathbb{R}^N$. A set $\mathcal{I}$ of rational invariants is separating on a subset $W \subset \mathbb{R}^N$ if W is contained in the domain of definition of each $I \in \mathcal{I}$ and $\forall w_1, w_2 \in W$*

$$I(w_1) = I(w_2), \quad \forall I \in \mathcal{I} \quad \Longleftrightarrow \quad \exists g \in G \text{ such that } w_1 = g \cdot w_2.$$

[3] Here $y = y^{(0)}$ and $J^0 = \mathbb{R}^2$.

[4] We note the duality of our view of variables $y^{(k)}$. On one hand, they are viewed as independent coordinate functions on J^n. On the other hand, the operator $\frac{d}{dx}$ is applied under assumption that y is a function of x and, therefore, $y^{(k)}$ is also viewed as the k-th derivative of y with respect to x. (The same duality of view appears in calculus of variations.)

Definition 14. (DIFFERENTIALLY SEPARATING SET) *Let r-dimensional algebraic group G act on $\mathbb{R}^2$. Let K and T be rational differential invariants of orders $r-1$ and r, respectively. The set $\mathcal{I} = \{K, T\}$ is called* differentially separating *if K separates orbits on Zariski open subset $W^{r-1} \subset J^{r-1}$ and $\mathcal{I} = \{K, T\}$ separates orbits on a Zariski open subset of $W^r \subset J^r$.*

4.2 Jets of curves and signatures

Let $\mathcal{X} \subset \mathbb{R}^2$ be defined by an implicit equation $F(x, y) = 0$. Then the derivatives of y with respect to x are rational functions on $\mathcal{X}$, computed using implicit differentiation. Namely, for $\mathbf{p} \in \mathcal{X}$:

$$\begin{aligned} y_{\mathcal{X}}^{(1)}(\mathbf{p}) &= -\frac{F_x(\mathbf{p})}{F_y(\mathbf{p})}, \\ y_{\mathcal{X}}^{(2)}(\mathbf{p}) &= \frac{-F_{xx}(\mathbf{p})\, F_y^2(\mathbf{p}) + 2\, F_{xy}(\mathbf{p})\, F_x(\mathbf{p})\, F_y(\mathbf{p}) - F_{yy}(\mathbf{p})\, F_x^2(\mathbf{p})}{F_y^3(\mathbf{p})}, \\ &\vdots \end{aligned} \tag{15}$$

Definition 15. *The n-th jet of a curve $\mathcal{X} \subset \mathbb{R}^2$ is a rational map $j_{\mathcal{X}}^n \colon \mathcal{X} \to J^n$, where for $\mathbf{p} \in \mathcal{X}$*

$$j_{\mathcal{X}}^n(\mathbf{p}) = \left(x(\mathbf{p}),\, y(\mathbf{p}),\, y_{\mathcal{X}}^{(1)}(\mathbf{p}), \ldots, y_{\mathcal{X}}^{(n)}(\mathbf{p})\right).$$

From (14) it follows that $$j_{g\cdot\mathcal{X}}^n(g \cdot \mathbf{p}) = g \cdot [j_{\mathcal{X}}^n(\mathbf{p})] \tag{16}$$

If $\mathcal{X}$ has a rational parameterization $\gamma(t) = \big(x(t),\, y(t)\big)$, then

$$y_{\mathcal{X}}^{(1)}\big(\gamma(t)\big) = \frac{\dot{y}}{\dot{x}} \quad \text{and} \quad y_{\mathcal{X}}^{(k)}\big(\gamma(t)\big) = \frac{\dot{y}^{(k-1)}}{\dot{x}}, \quad k = 2, \ldots \tag{17}$$

where $\dot{}$ here and below denotes the derivative with respect to the parameter. In this case, we view $j_{\mathcal{X}}^n$ as a rational function $\mathbb{R} \to J^n$.

Definition 16. *A restriction of a differential function $\Phi \colon J^n \to \mathbb{R}$ to a curve $\mathcal{X}$ is a composition of Φ with the n-th jet of curve, i. e. $\Phi|_{\mathcal{X}} = \Phi \circ j_{\mathcal{X}}^n \colon \mathcal{X} \to \mathbb{R}$.*

Definition 17. *Let $\mathcal{I} = \{K, T\}$ be a differentially separating set of invariants for the G-action (see Definition 14). Then a point $\mathbf{p} \in \mathcal{X}$ is called $\mathcal{I}$-regular if:*

(1) $\mathbf{p}$ is a non-singular point of $\mathcal{X}$;

(2) $j_{\mathcal{X}}^{r-1}(\mathbf{p}) \in W^{r-1}$ and $j_{\mathcal{X}}^r(\mathbf{p}) \in W^r$;

(3) $\left.\frac{\partial K}{\partial y^{(r-1)}}\right|_{j_{\mathcal{X}}^{r-1}(\mathbf{p})} \neq 0$ and $\left.\frac{\partial T}{\partial y^{(r)}}\right|_{j_{\mathcal{X}}^{r}(\mathbf{p})} \neq 0$.

An algebraic curve $\mathcal{X} \subset \mathbb{R}^2$ is called non-exceptional *with respect to $\mathcal{I}$ if all but a finite number of its points are $\mathcal{I}$-regular.*

Remark 18. *If $\mathcal{X}$ is a non-exceptional curve with respect to $\mathcal{I}$, then $K|_{\mathcal{X}}$ and $T|_{\mathcal{X}}$ are rational functions on $\mathcal{X}$. The $\mathcal{I}$-regular points of $\mathcal{X}$ are in the domain of the definition of these functions.*

Definition 19. (SIGNATURE) *Let $\mathcal{I} = \{K, T\}$ be differentially separating set of invariants with respect to G-action and $\mathcal{X}$ be a non-exceptional curve with respect to $\mathcal{I}$. The signature $\mathcal{S}_{\mathcal{X}}$ is the image of the rational map $S|_{\mathcal{X}}\colon \mathcal{X} \to \mathbb{R}^2$ defined by $S_{\mathcal{X}}(\mathbf{p}) = (K|_{\mathcal{X}}(\mathbf{p})\,,\, T|_{\mathcal{X}}(\mathbf{p}))$.* [5]

Remark 20. *Let $\mathcal{I} = \{K, T\}$ be a set of differentially separating invariants (see Definition 14). Let $\mathcal{X} \subset \mathbb{R}^2$ be a non $\mathcal{I}$-exceptional curve defined by an implicit equation $F(x, y) = 0$. Then $K|_{\mathcal{X}}(x, y) = \frac{k_1(x,y)}{k_2(x,y)}$, $T|_{\mathcal{X}} = \frac{t_1(x,y)}{t_2(x,y)}$, where k_1, k_2 and t_1, t_2 are pairs of polynomials with no non-constant common factors modulo F. Consider an ideal*

$$X := \langle F, k_2\,\varkappa - k_1,\, t_2\,\tau - t_1,\, k_2\,t_2\,\sigma - 1\rangle \subset \mathbb{R}[\varkappa, \tau, x, y, \sigma]. \tag{18}$$

The algebraic closure $\overline{\mathcal{S}_{\mathcal{X}}}$ of signature set $\mathcal{S}_{\mathcal{X}}$ is the variety of the elimination ideal $\hat{X} = X \cap \mathbb{R}[\varkappa, \tau]$.

Remark 21. *We note that $\dim \overline{\mathcal{S}_{\mathcal{X}}} = 0$ if and only if $K_{\mathcal{X}}$ and $T_{\mathcal{X}}$ are constant functions on $\mathcal{X}$ and $\dim \overline{\mathcal{S}_{\mathcal{X}}} = 1$ otherwise. In the latter case $\overline{\mathcal{S}_{\mathcal{X}}}$ is an algebraic planar curve with a single defining equation $\hat{S}_{\mathcal{X}}(\varkappa, \tau) = 0$. The equality of signatures for two curves, $\mathcal{S}_{\mathcal{X}_1} = \mathcal{S}_{\mathcal{X}_2}$, implies $\hat{S}_{\mathcal{X}_1}(\varkappa, \tau)$ is equal up to a constant multiple to $\hat{S}_{\mathcal{X}_2}(\varkappa, \tau)$. The converse, is not true over $\mathbb{R}$, because it is not an algebraically closed field, but is true over $\mathbb{C}$ (see [7]). This, in particular, makes an implementation of projection algorithms over real numbers more challenging.*

Theorem 22. (GROUP-EQUIVALENCE CRITERION) *Assume that algebraic curves $\mathcal{X}_1$ and $\mathcal{X}_2$ are non-exceptional with respect to differentially separating invariants $\mathcal{I} = (K, T)$ under G-action. Then $\mathcal{X}_1$ and $\mathcal{X}_2$ are G-equivalent if and only if their signatures are equal:*

$$\mathcal{X}_1 \cong_G \mathcal{X}_2 \quad\Longleftrightarrow\quad \mathcal{S}_{\mathcal{X}_1} = \mathcal{S}_{\mathcal{X}_2}.$$

Direction $\Longrightarrow$ follows immediately from the definition of invariants. Direction $\Longleftarrow$ is proved in Appendix 8.2.

Remark 23. *A definition of signature for sufficiently smooth non-algebraic curves appears, for instance, in [5] and is analogous to our Definition 19 (rationality of functions is no longer required). In the smooth case, the direction $\Longrightarrow$ of Theorem 22 is still valid, but the direction $\Longleftarrow$ is not. For example, curves $y = \cos(x), x \in [0, 2\pi]$, and $y = \sin(x), x \in [0, 2\pi]$, have the same Euclidean signatures, but are not equivalent under the action of Euclidean group. Counter-examples with closed curves and a discussion of the extend to which signature determines a smooth curve up to a group transformation can be found in [19].*

4.3 Separating sets of invariants for affine and projective actions

In this section, we construct a differentially separating set of rational invariants for affine and projective actions. We will build them from classical invariants from differential geometry. We start with Euclidean curvature[6] $\kappa = \frac{y^{(2)}}{(1+[y^{(1)}]^2)^{3/2}}$ which is, up to a sign[7], a differential invariant of the lowest order. Higher order Euclidean differential invariants are obtained by differentiating

[5] If $\mathcal{X}$ has a rational parameterization $\gamma\colon \mathbb{R} \to \mathbb{R}^2$, then $K|_{\mathcal{X}}$ and $T|_{\mathcal{X}}$ are rational functions from $\mathbb{R}$ to $\mathbb{R}$ and, therefore, $S_{\mathcal{X}}$ is a rational map from $\mathbb{R}$ to $\mathbb{R}^2$.

[6] For a parametric curve the formula $\kappa = \frac{\ddot{y}\dot{x} - \ddot{x}\dot{y}}{(\dot{x}^2+\dot{y}^2)^{3/2}}$ can be used.

[7] The sign of κ changes when a curve is reflected, rotated by π radians or traced in the opposite direction. A rational function κ^2 is invariant under the full Euclidean group.

the curvature with respect to the Euclidean arclength $ds = \sqrt{1+[y^{(1)}]^2}\,dx$, i. e. $\kappa_s = \frac{d\kappa}{ds} = \frac{1}{\sqrt{1+[y^{(1)}]^2}}\frac{d\kappa}{dx}$, $\kappa_{ss} = \frac{d\kappa_s}{ds}, \dots$.

Affine and projective curvatures and infinitesimal arclengths are well known, and can be expressed in terms of Euclidean invariants [8, 18]. In particular, $\mathcal{SA}$-curvature μ and infinitesimal $\mathcal{SA}$-arclength $d\alpha$ are expressed in terms of their Euclidean counterparts as follows:

$$\mu = \frac{3\,\kappa\,(\kappa_{ss} + 3\,\kappa^3) - 5\,\kappa_s^2}{9\,\kappa^{8/3}}, \quad d\alpha = \kappa^{1/3} ds. \tag{19}$$

By considering the effects of scalings and reflections on $\mathcal{SA}(2)$-invariants, we obtain two lowest order $\mathcal{A}(2)$-invariants:

$$K_{\mathcal{A}} = \frac{(\mu_\alpha)^2}{\mu^3}, \quad T_{\mathcal{A}} = \frac{\mu_{\alpha\alpha}}{3\,\mu^2}. \tag{20}$$

They are of order 5 and 6, respectively, and are *rational functions* in jet variables.[8]

$\mathcal{PGL}(3)$-curvature η and infinitesimal arclength $d\rho$ are expressed in terms of their $\mathcal{SA}$-counterparts:

$$\eta = \frac{6\mu_{\alpha\alpha\alpha}\mu_\alpha - 7\,\mu_{\alpha\alpha}^2 - 9\mu_\alpha^2\,\mu}{6\mu_\alpha^{8/3}}, \quad d\rho = \mu_\alpha^{1/3} d\alpha. \tag{21}$$

The two lowest order *rational* $\mathcal{PGL}(3)$-invariants are of differential order 7 and 8, respectively:[9]

$$K_{\mathcal{P}} = \eta^3, \quad T_{\mathcal{P}} = \eta_\rho. \tag{22}$$

Theorem 24. *(*DIFFERENTIALLY SEPARATING SETS OF AFFINE AND PROJECTIVE INVARIANTS.*) According to Definition 14:*

1. *The set $\mathcal{I}_{\mathcal{A}} = \{K_{\mathcal{A}}, T_{\mathcal{A}}\}$ given by (20) is differentially separating for the $\mathcal{A}(2)$-action (5) on $\mathbb{R}^2$.*
2. *The set $\mathcal{I}_{\mathcal{PGL}} = \{K_{\mathcal{P}}, T_{\mathcal{P}}\}$ given by (22) is differentially separating for the $\mathcal{PGL}(3)$-action (4) on $\mathbb{R}^2$.*

Proposition 25. *$\mathcal{I}_{\mathcal{A}}$-exceptional algebraic curves are lines and parabolas. $\mathcal{I}_{\mathcal{PGL}}$-exceptional algebraic curves are lines and conics.*

The proofs of Theorem 24 and Proposition 25 are given in Appendices 8.3 and 8.4, respectively.

Corollary 26. *An $\mathcal{I}_{\mathcal{A}}$-exceptional algebraic curve is* not *$\mathcal{A}(2)$ equivalent to a non $\mathcal{I}_{\mathcal{A}}$-exceptional algebraic curve. An $\mathcal{I}_{\mathcal{PGL}}$-exceptional algebraic curve is* not *$\mathcal{PGL}(3)$ equivalent to a non $\mathcal{I}_{\mathcal{PGL}}$-exceptional algebraic curve.*

Theorem 24, in combination with Theorem 22, leads to a solution for the projective and the affine equivalence problems for curves.

5 Algorithms and Examples

In this section, we outline the algorithms for solving projection problems based on a combination of the projection criteria of Section 3 and the group equivalence criterion of Section 4. For simplicity, we treat the case of rational algebraic curves, while the algorithms covering arbitrary algebraic curves are presented in Appendix 8.5.

[8] Explicit expressions of these invariants in terms of jet coordinates are given by formulas (26) in Appendix 8.1.

[9] Explicit expressions of these invariants in terms of jet coordinates are given by formulas (27) in Appendix 8.1.

5.1 Central projections.

The following algorithm is based on the central projection criteria stated in Theorem 8.

Algorithm 27. (Central projections.)

INPUT: Rational maps $\Gamma(s) = \big(z_1(s), z_2(s), z_3(s)\big)$, $s \in \mathbb{R}$ *and* $\gamma(t) = (x(t),\, y(t))$, $t \in \mathbb{R}$ *parametrizing algebraic curves* $\mathcal{Z} \subset \mathbb{R}^3$ *and* $\mathcal{X} \subset \mathbb{R}^2$.

OUTPUT: The truth of the statement: $\exists [P] \in \mathcal{CP},$ *such that* $\mathcal{X} = P(\mathcal{Z})$.

STEPS:

1. *if* $\mathcal{X}$ *is a line or a conic then follow a special procedure (Algorithm 38 in Appendix 8.6), else*
2. *evaluate* $\mathcal{PGL}(3)$*-invariants (22) on* $\mathcal{X}$. *Obtain two rational functions* $K_{\mathcal{P}}|_{\mathcal{X}}$ *and* $T_{\mathcal{P}}|_{\mathcal{X}}$ *of* t;
3. *for arbitrary* $c_1, c_2, c_3 \in \mathbb{R}$ *define a curve* $\tilde{\mathcal{Z}}_c$ *parametrized by* $\epsilon_c(s) = \Big(\frac{z_1(s)+c_1}{z_3(s)+c_3},\, \frac{z_2(s)+c_2}{z_3(s)+c_3}\Big)$;
4. *evaluate* $\mathcal{PGL}(3)$*-invariants (22) on* $\tilde{\mathcal{Z}}_c$. *Obtain two rational functions* $K_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}$ *and* $T_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}$ *of* c *and* s;
5. *determine the truth of the statement:*

$$\exists c \in \mathbb{R}^3 \quad \forall s \in \mathbb{R} \quad \exists t \in \mathbb{R} \quad K_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}(c,\, s) = K_{\mathcal{P}}|_{\mathcal{X}}(t) \ \textit{and}\ T_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}(c,\, s) = T_{\mathcal{P}}|_{\mathcal{X}}(t).$$

If the output is TRUE then, in many cases, we can, in addition to establishing the existence of c_1, c_2, c_3 in Step 5 of the algorithm, find at least one of such triplets explicitly. We then know that $\mathcal{Z}$ can be projected to $\mathcal{X}$ by a projection centered at $(-c_1, -c_2, -c_3)$. We can also, in many cases, determine explicitly a transformation $[A] \in \mathcal{PGL}(3)$ that maps $\mathcal{X}$ to $\tilde{\mathcal{Z}}_c$. We then know that $\mathcal{Z}$ can be projected to $\mathcal{X}$ by the projection $[P] = [A][P^0_{\mathcal{C}}][B]$, where $P^0_{\mathcal{C}}$ and B are defined by (8).

Example 28. *We would like to decide if the spatial curve* $\mathcal{Z}$ *parametrized by* $\Gamma(s) = \big(s^3,\, s^2,\, s\big)$, $s \in \mathbb{R}$ *projects to any of the three given planar curves* $\mathcal{X}_1$, $\mathcal{X}_2$, $\mathcal{X}_3$ *and* $\mathcal{X}_4$ *parametrized, respectively, by:*

$$\gamma_1(t) = \big(t^2\,,\, t\big)\,, \quad \gamma_2(t) = \left(\frac{t^3}{t+1}\,,\, \frac{t^2}{t+1}\right), \quad \gamma_3(t) = \left(\frac{t}{t^3+1}\,,\, \frac{t^2}{t^3+1}\right), \quad \gamma_4(t) = \big(t,\, t^5\big)\,.$$

For $c_1, c_2, c_3 \in \mathbb{R}$ *define a curve* $\tilde{\mathcal{Z}}_c$ *parametrized by* $\epsilon_c(s) = \Big(\frac{s^3+c_1}{s+c_3},\, \frac{s^2+c_2}{s+c_3}\Big)$.

Note that $\mathcal{X}_1$ *is parabola and so is* $\mathcal{PGL}(3)$*-exceptional. It is known that all planar conics are* $\mathcal{PGL}(3)$*-equivalent and so, from Theorem 8, we know that* $\mathcal{Z}$ *can be projected on* $\mathcal{X}_1$ *if there exist* $c \in \mathbb{R}^3$, *such that the curve* $\tilde{\mathcal{Z}}_c$ *is a conic. This is obviously true for* $c_1 = c_2 = c_3 = 0$. *Indeed, one can check that* $\mathcal{Z}$ *can be projected to* $\mathcal{X}_1$ *by projection* $x = \frac{z_1}{z_3}$, $y = \frac{z_2}{z_3}$.

The curve $\mathcal{X}_2$ *is not* $\mathcal{PGL}(3)$*-exceptional. It has a constant signature map:*

$$K_{\mathcal{P}}|_{\mathcal{X}_2}(t) \equiv \frac{250047}{12800} \ \textit{and}\ T_{\mathcal{P}}|_{\mathcal{X}_2}(t) \equiv 0, \quad \forall t \in \mathbb{R}.$$

Following Algorithm 27, we need to decide whether there exist $c_1, c_2, c_3 \in \mathbb{R}$, *such that* $K_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}(s) = \frac{250047}{12800}$ *and* $T_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}(s) = 0$, $\forall s \in \mathbb{R}$. *This is, indeed, true for* $c_1 = c_2 = 0$ *and* $c_3 = 1$. *We conclude that* $\mathcal{Z}$ *can be projected to* $\mathcal{X}_2$. *It is not difficult to find a possible projection:* $x = \frac{z_1}{z_3+1}$, $y = \frac{z_2}{z_3+1}$.

The curve $\mathcal{X}_3$ has a non-constant signature map:

$$K_{\mathcal{P}}|_{\mathcal{X}_3}(t) = -\frac{9261}{50}\,\frac{t^7 - t^4 + t}{(t^3-1)^8} \text{ and } T_{\mathcal{P}}|_{\mathcal{X}_3}(t) = -\frac{21}{10}\,\frac{(t^3+1)^4}{(t^3-1)^4}.$$

Evaluation of step 5 of Algorithm 27 yields TRUE (one can, in fact, check that for $c_1 = 0, c_2 = 0, c_3 = 1$ it is true that $K_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}(s) = K_{\mathcal{P}}|_{\mathcal{X}_3}(s)$ and $T_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}(s) = K_{\mathcal{P}}|_{\mathcal{X}_3}(s)$, $\forall s \in \mathbb{R}$). We conclude that $\mathcal{Z}$ can be projected to $\mathcal{X}_3$. It is not difficult to determine a possible projection: $x = \frac{z_3}{z_1+1}$, $y = \frac{z_2}{z_1+1}$.

It is important to observe that although $\mathcal{Z}$ can be projected to each of the planar curves $\mathcal{X}_1$, $\mathcal{X}_2$, and $\mathcal{X}_3$, these planar curves are not *$\mathcal{PGL}(3)$-equivalent. This underscores an observation made in Remark 7.*

The curve $\mathcal{X}_4$ has a constant signature map: $K_{\mathcal{P}}|_{\mathcal{X}_3}(t) \equiv \frac{1029}{128}$ and $T_{\mathcal{P}}|_{\mathcal{X}_3}(t) \equiv 0$. Following Algorithm 27, we need to decide whether there exist $c_1, c_2, c_3 \in \mathbb{R}$, such that $K_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}(s) = \frac{1029}{128}$ and $T_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}(s) = 0$, $\forall s \in \mathbb{R}$. Substitution of several values of s, yields a system of polynomial equations for $c_1, c_2, c_3 \in \mathbb{R}$ that has no solutions. We conclude that there is no central projection from $\mathcal{Z}$ to $\mathcal{X}_4$.

5.2 Parallel projections

The following algorithm is based on the reduced parallel projection criteria stated in Corollary 10.

Algorithm 29. (Parallel projections.)
INPUT: Rational maps $\Gamma(s) = \big(z_1(s), z_2(s), z_3(s)\big)$, $s \in \mathbb{R}$ and $\gamma(t) = (x(t), y(t))$, $t \in \mathbb{R}$ parametrizing algebraic curves $\mathcal{Z} \subset \mathbb{R}^3$ and $\mathcal{X} \subset \mathbb{R}^2$.
OUTPUT: The truth of the statement: $\exists [P] \in \mathcal{PP}$, such that $\mathcal{X} = P(\mathcal{Z})$.
STEPS:

1. *if $\mathcal{X}$ is a line or a parabola then follow a special procedure (Algorithm 40 in Appendix 8.6), else*
2. *evaluate $\mathcal{A}(2)$-invariants (20) on $\mathcal{X}$. Obtain two rational functions $K_{\mathcal{A}}|_{\mathcal{X}}$ and $K_{\mathcal{A}}|_{\mathcal{X}}$ of t;*
3. *define a curve $\tilde{\mathcal{Z}}$ parametrized by $\alpha(s) = (z_2(s), z_3(s))$;*
4. *evaluate $\mathcal{A}(2)$-invariants (20) on $\tilde{\mathcal{Z}}$. Obtain two rational functions $K_{\mathcal{A}}|_{\tilde{\mathcal{Z}}}$ and $T_{\mathcal{A}}|_{\tilde{\mathcal{Z}}}$ of s;*
5. *determine the truth of the statement:*

   $$\forall s \in \mathbb{R} \quad \exists t \in \mathbb{R} \quad K_{\mathcal{A}}|_{\tilde{\mathcal{Z}}}(s) = K_{\mathcal{A}}|_{\mathcal{X}}(t) \text{ and } T_{\mathcal{A}}|_{\tilde{\mathcal{Z}}}(s) = T_{\mathcal{A}}|_{\mathcal{X}}(t).$$

   If TRUE *exit the procedure, else*
6. *for arbitrary $b \in \mathbb{R}$, define a curve $\tilde{\mathcal{Z}}_b$ parametrized by $\beta_b(s) = (z_1(s) + b\, z_2(s),\, z_3(s))$;*
7. *evaluate $\mathcal{A}(2)$-invariants (20) on $\tilde{\mathcal{Z}}_b$. Obtain two rational functions $K_{\mathcal{A}}|_{\tilde{\mathcal{Z}}_b}(b,s)$ and $T_{\mathcal{A}}|_{\tilde{\mathcal{Z}}_b}(b,s)$ of b and s;*
8. *determine the truth of the statement:*

   $$\exists b \in \mathbb{R} \quad \forall s \in \mathbb{R} \quad \exists t \in \mathbb{R} \quad K_{\mathcal{A}}|_{\tilde{\mathcal{Z}}_b}(b,\, s) = K_{\mathcal{A}}|_{\mathcal{X}}(t) \text{ and } T_{\mathcal{A}}|_{\tilde{\mathcal{Z}}_b}(b,\, s) = T_{\mathcal{A}}|_{\mathcal{X}}(t).$$

   If TRUE *exit the procedure, else*
9. *for arbitrary $a \in \mathbb{R}^2$, define a curve $\tilde{\mathcal{Z}}_a$ parametrized by $\delta_a(s) = (z_1(s) + a_1\, z_3(s),\, z_2 + a_2\, z_3(s))$;*

10. *evaluate $\mathcal{A}(2)$-invariants (20) on $\tilde{\mathcal{Z}}_a$. Obtain two rational functions $K_\mathcal{A}|_{\tilde{\mathcal{Z}}_a}(a,s)$ and $T_\mathcal{A}|_{\tilde{\mathcal{Z}}_a}(a,s)$ of a_1, a_2 and s;*
11. *determine the truth of the statement:*

$$\exists a \in \mathbb{R}^2 \quad \forall s \in \mathbb{R} \quad t \in \mathbb{R} \quad K_\mathcal{A}|_{\tilde{\mathcal{Z}}_a}(a,\, s) = K_\mathcal{A}|_\mathcal{X}(t) \text{ and } T_\mathcal{A}|_{\tilde{\mathcal{Z}}_a}(a,\, s) = T_\mathcal{A}|_\mathcal{X}(t).$$

Example 30. *To decide whether the spatial curve $\mathcal{Z}$ parametrized by $\Gamma(s) = (z_1(s),\, z_2(s),\, z_3(s)) = \left(s^4+1,\, s^2,\, s\right)$, $s \in \mathbb{R}$, can be projected to $\mathcal{X}$ parametrized by $\gamma(t) = \left(t\,,\, t^4+t^2\right)$, $t \in \mathbb{R}$ by a parallel projection, we start by noticing that $\mathcal{X}$ is not an $\mathcal{A}(2)$-exceptional curve. Its signature map is given by non-constant rational functions: $T_\mathcal{A}|_\mathcal{X}(t) = \frac{100\,t^2\,(3-14\,t^2)^2}{(1-14\,t^2)^3}$, $\quad K_\mathcal{A}|_\mathcal{X}(t) = \frac{-5\,(140\,t^4-56\,t^2+1)}{(1-14\,t^2)^2}$.*

Following Algorithm 29, we first check whether $\mathcal{X}$ is $\mathcal{A}(2)$-equivalent to $\tilde{\mathcal{Z}}$ parametrized by $\alpha(s) = (z_2(s),\, z_3(s)) = \left(s^2,\, s\right)$. The answer is no, since $\tilde{\mathcal{Z}}$ is an $\mathcal{A}(2)$-exceptional curve (parabola) and $\mathcal{X}$ is not $\mathcal{A}(2)$-exceptional. We next check whether there exists $b \in \mathbb{R}$ such that $\mathcal{X}$ is $\mathcal{A}(2)$-equivalent to $\tilde{\mathcal{Z}}_b$ parametrized by $\beta_b(s) = \left(\, z_1(s) + b\, z_2(s),\, z_3(s)\right) = \left(s^4+1+b\,s^2,\, s\right)$. We evaluate invariants (20) on $\tilde{\mathcal{Z}}_b$: $T_\mathcal{A}|_{\tilde{\mathcal{Z}}_b}(b,s) = \frac{100\,s^2\,(3\,b-14s^2)^2}{(b-14s^2)^3}$, $\quad K_\mathcal{A}|_{\tilde{\mathcal{Z}}_b}(b,s) = \frac{-5\,(140\,s^4-56\,b\,s^2+b^2)}{(b-14\,s^2)^2}$. Since $T_\mathcal{A}|_{\tilde{\mathcal{Z}}_b}(1,s) = K_\mathcal{A}|_\mathcal{X}$ and $T_\mathcal{A}|_{\tilde{\mathcal{Z}}_b}(1,s) = T_\mathcal{A}|_\mathcal{X}$, we conclude that $\tilde{\mathcal{Z}}_{b=1}$ is $\mathcal{A}(2)$-equivalent to $\mathcal{X}$ and, therefore, $\mathcal{Z}$ projects to $\mathcal{X}$ by a parallel projection.

Example 31. *We would like to decide if the spatial curve $\mathcal{Z}$ parametrized by $(z_1(s),\, z_2(s), z_3(s)) = \left(s^2+s,\, s^3-3\,s^2,\, s^4\right)$, $s \in \mathbb{R}$, projects to any of the three given planar curves $\mathcal{X}_1$, $\mathcal{X}_2$ and $\mathcal{X}_3$ parametrized, respectively, by:*

$$\gamma_1(t) = \left(t^4+t\,, \quad t^2\right), \quad \gamma_2(t) = \left(t^3-t\,, \quad t^3+t^2\right), \quad \gamma_3(t) = \left(\frac{t}{(1+t^3)}, \quad \frac{t^2}{(1+t^3)}\right).$$

Following Algorithm 29, we establish that $\tilde{\mathcal{Z}}$ parametrized by $\alpha(s) = \left(z_2(s), z_3(s)\right)$ and $\tilde{\mathcal{Z}}_b$ parametrized by $\beta_b(s) = \left(\, z_1(s) + b\, z_2(s),\, z_3(s)\right)$, for all $b \in \mathbb{R}$, are not $\mathcal{A}(2)$-equivalent to either of $\mathcal{X}$'s. We then establish that $\tilde{\mathcal{Z}}_a$ parametrized by $\delta_a(s) = \left(z_1(s) + a_1\, z_3(s),\, z_2(s) + a_2\, z_3(s)\right)$ is $\mathcal{A}(2)$-equivalent to $\mathcal{X}_1$ when $a_1 = 0$ and $a_2 = 1/2$ and is $\mathcal{A}(2)$-equivalent to $\mathcal{X}_2$ when $a_1 = 0$ and $a_2 = 0$, but there are no real values of a_1 and a_2 such that $\tilde{\mathcal{Z}}_a$ and $\mathcal{X}_3$ are $\mathcal{A}(2)$-equivalent.

We conclude that there are parallel projections of $\mathcal{Z}$ to both $\mathcal{X}_1$ and $\mathcal{X}_2$, but not to $\mathcal{X}_3$. Note that $\mathcal{X}_1$ and $\mathcal{X}_2$ are not $\mathcal{A}(2)$-equivalent because (their affine signatures have different implicit equations). This underscores an observation made in Remark 7.

6 Projection of finite ordered sets (lists) of points

In [1, 2], the authors present a solution to the problem of deciding whether or not there exists a parallel projection of a list $Z = (\mathbf{z}^1, \ldots, \mathbf{z}^m)$ of m points in $\mathbb{R}^3$ to a list $X = (\mathbf{x}^1, \ldots, \mathbf{x}^m)$ of m points in $\mathbb{R}^2$, without finding a projection explicitly. They identify the lists Z and X with the elements of certain Grassmanian spaces and use Plüker embedding of Grassmanians into projective spaces to explicitly define the algebraic variety that characterizes pairs of sets related by an prallel projection.

We indicate here how our approach leads to an alternative solution for the projection problem for lists of points. Details of this adaptation appear in the dissertation [4].

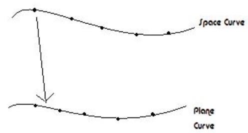

Figure 1: Projection problem for curves vs. projection problems for lists of points

Theorem 32. *(*CENTRAL PROJECTION CRITERIA FOR LISTS OF POINTS.*) A given list $Z = (\mathbf{z}^1, \dots, \mathbf{z}^m)$ of m points in $\mathbb{R}^3$ with coordinates $\mathbf{z}^l = (z_1^l, z_2^l, z_3^l)$, $l = 1 \dots m$, projects onto a given list $X = (\mathbf{x}^1, \dots, \mathbf{x}^m)$ of m points in $\mathbb{R}^2$ with coordinates $\mathbf{x}^l = (x^l, y^l)$, $l = 1 \dots m$, by a central projection if and only if there exist $c_1, c_2, c_3 \in \mathbb{R}$ and $[A] \in \mathcal{PGL}(3)$, such that*

$$[x^l, y^l, 1]^{\mathrm{T}} = [A][z_1^l + c_1,\, z_2^l + c_2,\, z_3^l + c_3]^{\mathrm{T}} \text{ for } l = 1 \dots m. \tag{23}$$

Theorem 33. *(*PARALLEL PROJECTION CRITERIA FOR LISTS OF POINTS.*) A given list $Z = (\mathbf{z}^1, \dots, \mathbf{z}^m)$ of m points in $\mathbb{R}^3$ with coordinates $\mathbf{z}^l = (z_1^l, z_2^l, z_3^l)$, $l = 1 \dots m$, projects onto a given list $X = (\mathbf{x}^1, \dots, \mathbf{x}^m)$ of m points in $\mathbb{R}^2$ with coordinates $\mathbf{x}^l = (x^l, y^l)$, $l = 1 \dots m$, by a parallel projection if and only if there exist $c_1, c_2 \in \mathbb{R}$, an ordered triplet $(i, j, k) \in \{(1,2,3),\, (1,3,2),\, (2,3,1)\}$ and $[A] \in \mathcal{A}(2)$, such that*

$$[x^l, y^l, 1]^{\mathrm{T}} = [A]\left[z_i^l + c_1\, z_k^l,\, z_j^l + c_2\, z_k^l, 1\right]^{\mathrm{T}} \text{ for } l = 1 \dots m. \tag{24}$$

The proofs of Theorems 32 and 33 are straightforward adaptations of the proofs of Theorems 8 and 9. The reduced parallel projection criteria for curves, given in Corollary 10, is adapted to the finite lists in an analogous way.

The central and the parallel projection problems for lists of m points is therefore reduced to a modification of the problems of equivalence of two lists of m points in $\mathbb{PR}^2$ under the action of $\mathcal{PGL}(3)$ and $\mathcal{A}(2)$ groups, respectively. A separating set of invariants for lists of m points in $\mathbb{PR}^2$ under $\mathcal{A}(2)$-action consists of ratios of certain areas and is listed, for instance, in Theorem 3.5 of [20]. Similarly, a separating set of invariants for lists of m ordered points in $\mathbb{PR}^2$ under $\mathcal{PGL}(3)$-action consists of cross-ratios of certain areas and is listed, for instance, in Theorem 3.10 in [20]. In the case of central projections we, therefore, obtain a system of polynomial equations on c_1, c_2 and c_3 that have solutions if and only if the given set Z projects to the given set X and analog of Algorithms 27 follows. The parallel projections are treated in a similar way.

Figure 1 illustrates that a solution of the projection problem for lists of points does not provide an immediate solution to the discretization of the projection problem for curves. Indeed, let $Z = (\mathbf{z}^1, \dots, \mathbf{z}^m)$ be a discrete sampling of a spatial curve $\mathcal{Z}$ and $X = (\mathbf{x}^1, \dots, \mathbf{x}^m)$ be a discrete sampling of a planar curve $\mathcal{X}$. It might be impossible to project the list Z onto X, even when the curve $\mathcal{Z}$ can be projected to the curve $\mathcal{X}$. Some approaches to the discretization of the projection algorithms for curves are discussed in the next section.

7 Directions of further research

The projection criteria developed in Section 3 reduce the problem of object-image correspondence for curves under a projection from $\mathbb{R}^3$ to $\mathbb{R}^2$ to a variation of the group-equivalence problem for

curves in $\mathbb{R}^2$. We use differential signature construction [5] to address the group-equivalence problem. In practical applications, curves are often given by samples of points. In this case, invariant numerical approximations of differential invariants presented in [3, 5] may be used to obtain signatures. Differential invariants and their approximations are highly sensitive to image perturbations and, therefore, are not practical in many situations. Other types of invariants, such as semi-differential (or joint) invariants [20, 23], integral invariants [10, 13, 21] and moment invariants [17] are less sensitive to image perturbations and may be employed to solve the group-equivalence problem.

One of the essential contributions of [1, 2] is the definition of an object/image distance between ordered sets of m points in $\mathbb{R}^3$ and $\mathbb{R}^2$, such that the distance is zero if and only if these sets are related by a projection. Since, in practice, we are given only an approximate position of points, a "good" object/image distance provides a tool for deciding whether a given set of points in $\mathbb{R}^2$ is a good approximation of a projection of a given set of points in $\mathbb{R}^3$. Defining such object/image distance in the case of curves is an important direction of further research.

8 Appendix

8.1 Explicit formulas for invariants

Let

$$\Delta_1 = 3\,y^{(4)}\,y^{(2)} - 5\,[y^{(3)}]^2 \text{ and } \Delta_2 = 9\,y^{(5)}\,[y^{(2)}]^2 - 45\,y^{(4)}\,y^{(3)}\,y^{(2)} + 40\,[y^{(3)}]^3. \tag{25}$$

The explicit formulas for the differentially separating set of rational $\mathcal{A}(2)$-invariants (20) are:

$$\begin{aligned} K_{\mathcal{A}} &= \frac{(\Delta_2)^2}{(\Delta_1)^3}; \qquad (26)\\ T_{\mathcal{A}} &= \frac{9\,y^{(6)}\,[y^{(2)}]^3 - 63\,y^{(5)}\,y^{(3)}\,[y^{(2)}]^2 - 45\,[y^{(4)}]^2\,[y^{(2)}]^2 + 255\,y^{(4)}\,[y^{(3)}]^2\,y^{(2)} - 160\,[y^{(3)}]^4}{(\Delta_1)^2}. \end{aligned}$$

The explicit formulas for the differentially separating set of rational $\mathcal{PGL}(3)$-invariants (22) are:

$$\begin{aligned} K_{\mathcal{P}} &= \frac{729}{8\,(\Delta_2)^8}\Big(18\,y^{(7)}\,[y^{(2)}]^4\;\Delta_2 - 189\,[y^{(6)}]^2\,[y^{(2)}]^6 \qquad (27)\\ &+ 126\,y^{(6)}\,[y^{(2)}]^4\;(9\,y^{(5)}\,y^{(3)}\,y^{(2)} + 15\,[y^{(4)}]^2\,y^{(2)} - 25\,y^{(4)}\,[y^{(3)}]^2)\\ &- 189\,[y^{(5)}]^2\,[y^{(2)}]^4\;(4\,[y^{(3)}]^2 + 15\,y^{(2)}\,y^{(4)})\\ &+ 210\,y^{(5)}\,y^{(3)}\,[y^{(2)}]^2\;(63\,[y^{(4)}]^2\,[y^{(2)}]^2 - 60\,y^{(4)}\,[y^{(3)}]^2\,y^{(2)} + 32\,[y^{(3)}]^4)\\ &- 525\,y^{(4)}y^{(2)}\;(9\,[y^{(4)}]^3\,[y^{(2)}]^3 + 15\,[y^{(4)}]^2\,[y^{(3)}]^2\,[y^{(2)}]^2 - 60\,y^{(4)}\,[y^{(3)}]^4\,y^{(2)} + 64\,[y^{(3)}]^6)\\ &+ 11200\,[y^{(3)}]^8\Big)^3; \end{aligned}$$

$$
\begin{aligned}
T_{\mathcal{P}} \;=\; & \frac{243\,[y^{(2)}]^4}{2\,(\Delta_2)^4}\,\Big(2\,y^{(8)}\,y^{(2)}\,(\Delta_2)^2 \\
- \;& 8\,y^{(7)}\,\Delta_2\,(9\,y^{(6)}\,[y^{(2)}]^3 - 36\,y^{(5)}\,y^{(3)}\,[y^{(2)}]^2 - 45\,[y^{(4)}]^2\,[y^{(2)}]^2 + 120\,y^{(4)}\,[y^{(3)}]^2\,y^{(2)} - 40\,[y^{(3)}]^4) \\
+ \;& 504\,[y^{(6)}]^3\,[y^{(2)}]^5 - 504\,[y^{(6)}]^2\,[y^{(2)}]^3\,(9\,y^{(5)}\,y^{(3)}\,y^{(2)} + 15\,[y^{(4)}]^2\,y^{(2)} - 25\,y^{(4)}\,[y^{(3)}]^2) \\
+ \;& 28\,y^{(6)}\,\big(432\,[y^{(5)}]^2\,[y^{(3)}]^2\,[y^{(2)}]^3 + 243\,[y^{(5)}]^2\,y^{(4)}\,[y^{(2)}]^4 - 1800\,y^{(5)}\,y^{(4)}\,[y^{(3)}]^3\,[y^{(2)}]^2 \\
- \;& 240y^{(5)}\,[y^{(3)}]^5\,y^{(2)} + 540y^{(5)}\,[y^{(4)}]^2\,[y^{(3)}]\,[y^{(2)}]^3 + 6600\,[y^{(4)}]^2\,[y^{(3)}]^4\,y^{(2)} - 2000y^{(4)}\,[y^{(3)}]^6 \\
- \;& 5175\,[y^{(4)}]^3\,[y^{(3)}]^2\,[y^{(2)}]^2 + 1350\,[y^{(4)}]^4\,[y^{(2)}]^3\big) - 2835\,[y^{(5)}]^4\,[y^{(2)}]^4 \\
+ \;& 252\,[y^{(5)}]^3 y^{(3)}\,[y^{(2)}]^2\,(9y^{(4)}\,y^{(2)} - 136\,[y^{(3)}]^2) - 35840\,[y^{(5)}]^2\,[y^{(3)}]^6 \\
- \;& 630\,[y^{(5)}]^2\,[y^{(4)}]\,[y^{(2)}]\,(69\,[y^{(4)}]^2\,[y^{(2)}]^2 - 160\,[y^{(3)}]^4 - 153\,y^{(4)}\,[y^{(3)}]^2\,[y^{(2)}]) \\
+ \;& 2100\,y^{(5)}\,[y^{(4)}]^2\,y^{(3)}\,(72\,[y^{(3)}]^4 + 63\,[y^{(4)}]^2\,[y^{(2)}]^2 - 193\,y^{(4)}\,[y^{(3)}]^2\,y^{(2)}) \\
- \;& 7875\,[y^{(4)}]^4\,(8\,[y^{(4)}]^2\,[y^{(2)}]^2 - 22y^{(4)}\,[y^{(3)}]^2\,[y^{(2)}] + 9\,[y^{(3)}]^4)\Big)\,.
\end{aligned}
$$

Remark 34. *If Δ_1 is zero at more than at a finite number of points of an algebraic curve $\mathcal{X}$ then $\mathcal{X}$ is either a line or a parabola, and then $\Delta_1 \equiv 0$. If Δ_2 is zero in more than at a finite number of points of $\mathcal{X}$ then $\mathcal{X}$ is either a line or a conic and then $\Delta_2 \equiv 0$.*

8.2 Proof of Theorem 22.

Direction $\Longrightarrow$ follows immediately from the definition of invariants. Below we prove $\Longleftarrow$. We notice that there are two cases. Either $K|_{\mathcal{X}_1}$ and $K|_{\mathcal{X}_2}$ are constant maps on $\mathcal{X}_1$ and $\mathcal{X}_2$, respectively, and these maps take the same value. Otherwise both $K|_{\mathcal{X}_1}$ and $K|_{\mathcal{X}_2}$ are non-constant rational maps on $\mathcal{X}_1$ and $\mathcal{X}_2$, respectively.

Case 1: There exists $c \in \mathbb{R}$ such that $K|_{\mathcal{X}_1}(\mathbf{p}_1) = c$ and $K_{\mathcal{X}_2}(\mathbf{p}_2) = c$ for all $\mathbf{p}_1 \in \mathcal{X}_1$ and for all $\mathbf{p}_2 \in \mathcal{X}_2$. Since $\mathcal{X}_1$ and $\mathcal{X}_2$ are non-exceptional, we may fix $\mathcal{I}_G$-regular points $\mathbf{p}_1 = (x_1, y_1) \in \mathcal{X}_1$ and $\mathbf{p}_2 = (x_2, y_2) \in \mathcal{X}_2$. Then, due to separation property of the invariant K, $\exists g \in G$ such that $j^{r-1}_{\mathcal{X}_1}(\mathbf{p}_1) = g \cdot [j^{r-1}_{\mathcal{X}_2}(\mathbf{p}_2)]$. We consider a new algebraic curve $\mathcal{X}_3 = g \cdot \mathcal{X}_2$. Then due to (16), we have

$$j^{r-1}_{\mathcal{X}_1}(\mathbf{p}_1) = j^{r-1}_{\mathcal{X}_3}(\mathbf{p}_1) =: \mathbf{p}^{(r-1)}. \tag{28}$$

Since $\mathbf{p}_1$ is a $\mathcal{I}$-regular point of $\mathcal{X}_1$, it follows from (28) that it is also a $\mathcal{I}$-regular point of $\mathcal{X}_3$ and, in particular, is non-singular. Let $F_1(x, y) = 0$ and $F_3(x, y) = 0$ be implicit equations of $\mathcal{X}_1$ and $\mathcal{X}_3$ repsectively. We may assume that $\frac{\partial F_1}{\partial y}(\mathbf{p}_1) \neq 0$ and $\frac{\partial F_3}{\partial y}(\mathbf{p}_1) \neq 0$ (otherwise, $\frac{\partial F_1}{\partial x}(\mathbf{p}_1) \neq 0$ and $\frac{\partial F_3}{\partial x}(\mathbf{p}_1) \neq 0$ and we may use a similar argument). Then, there exist functions $f_1(x)$ and $f_3(x)$, analytic on an interval $I \ni x_1$, such that $F_1(x, f_1(x)) = 0$ and $F_3(x, f_3(x)) = 0$ for $x \in I_1$.

Functions $y = f_1(x)$ and $y = f_3(x)$ are local analytic solutions of differential equation

$$K(x, y, y^{(1)}, \ldots, y^{(r-1)}) = c \tag{29}$$

with the same initial condition $f_1^{(k)}(x_1) = f_3^{(k)}(x_1)$, $k = 0, \ldots, r-1$ prescribed by (28). From the $\mathcal{I}$-regularity of $\mathbf{p}_1$, we have that $\left.\frac{\partial K}{\partial y^{(r-1)}}\right|_{\mathbf{p}^{(r-1)}} \neq 0$ and so (29) can be solved for $y^{(r-1)}$:

$$y^{(r-1)} = H(x, y, y^{(1)}, \ldots, y^{(r-2)}), \tag{30}$$

where function H is smooth in a neighborhood $\mathbf{p}^{(r-1)} \in J^{r-1}$. From the uniqueness theorem for the solutions of ODEs, it follows that $f_1(x) = f_3(x)$ on an interval $I \ni x_1$. Since $\mathcal{X}_1$ and $\mathcal{X}_3$ are irreducible algebraic curves it follows that $\mathcal{X}_1 = \mathcal{X}_3$. Therefore, $\mathcal{X}_1 = g \cdot \mathcal{X}_2$.

Case 2: $K|_{\mathcal{X}_1}$ and $K|_{\mathcal{X}_2}$ are non-constant rational maps. Then $\mathcal{S}_{\mathcal{X}_1} = \mathcal{S}_{\mathcal{X}_2}$ is a one-dimesional set that we will denote $\mathcal{S}$. Let $\hat{S}(\varkappa, \tau) = 0$ be the implicit equation for $\mathcal{S}$ (see Remark 20). We know that $\frac{\partial \hat{S}}{\partial \tau}(\varkappa, \tau) \neq 0$ for all but finite number of values $(\varkappa, \tau)$, because, otherwise, $K|_{\mathcal{X}_1}$ and $K|_{\mathcal{X}_2}$ are constant maps and the set $\mathcal{S}$ is zero-dimenional. Therefore, since the curves are non-exceptional, there exists $\mathcal{I}$-regular points $\mathbf{p}_1 = (x_1, y_1) \in \mathcal{X}_1$ and $\mathbf{p}_2 = (x_2, y_2) \in \mathcal{X}_2$ such that

$$K|_{\mathcal{X}_1}(\mathbf{p}_1) = K|_{\mathcal{X}_2}(\mathbf{p}_2) =: \varkappa_0, \quad T|_{\mathcal{X}_1}(\mathbf{p}_1) = T|_{\mathcal{X}_2}(\mathbf{p}_2) =: \tau_0 \text{ and } \frac{\partial \hat{S}}{\partial \tau}(\varkappa_0, \tau_0) \neq 0. \tag{31}$$

Due to separation property of the set $\mathcal{I}_G = \{K, T\}$, $\exists g \in G$ such that $j^r_{\mathcal{X}_1}(\mathbf{p}_1) = g \cdot [j^r_{\mathcal{X}_2}(\mathbf{p}_2)]$. We consider a new algebraic curve $\mathcal{X}_3 = g \cdot \mathcal{X}_2$. Then due to (16), we have

$$j^r_{\mathcal{X}_1}(\mathbf{p}_1) = j^r_{\mathcal{X}_3}(\mathbf{p}_1) =: \mathbf{p}^{(r)}. \tag{32}$$

From (31), (32) and $\mathcal{I}$-regularity of the point $\mathbf{p}_1 \in \mathcal{X}_1$ it follows that

$$K(\mathbf{p}^{(r)}) = \varkappa_0, \quad T(\mathbf{p}^{(r)}) = \tau_0 \text{ and } \left.\frac{\partial T}{\partial y^{(r)}}\right|_{\mathbf{p}^{(r)}} \neq 0 \tag{33}$$

Since $\mathbf{p}_1$ is a $\mathcal{I}$-regular point of $\mathcal{X}_1$, it follows from (32) that it is also a $\mathcal{I}$-regular point of $\mathcal{X}_3$ and, in particular, is non-singular. Let $F_1(x, y) = 0$ and $F_3(x, y) = 0$ be implicit equations of $\mathcal{X}_1$ and $\mathcal{X}_3$ repsectively. We may assume that $\frac{\partial F_1}{\partial y} \neq 0$ and $\frac{\partial F_3}{\partial y} \neq 0$ (otherwise, $\frac{\partial F_1}{\partial x} \neq 0$ and $\frac{\partial F_3}{\partial x} \neq 0$ and we may use a similar argument). Then, there exist functions $f_1(x)$ and $f_3(x)$, analytic on an interval $I \ni x_1$, such that $F_1(x, f_1(x)) = 0$ and $F_3(x, f_3(x)) = 0$ for $x \in I_1$.

Then functions $y = f_1(x)$ and $y = f_3(x)$ are local analytic solutions of differential equation

$$\hat{S}\left(K(x, y, y^{(1)}, \ldots, y^{(r-1)}), T(x, y, y^{(1)}, \ldots, y^{(r)})\right) = 0 \tag{34}$$

with the same initial condition $f_1^{(k)}(x_1) = f_3^{(k)}(x_1)$, $k = 0, \ldots, r$, dictated by (32).

Since $\frac{\partial \hat{S}}{\partial \tau}(\varkappa_0, \tau_0) \neq 0$ and $\left.\frac{\partial T}{\partial y^{(r)}}\right|_{\mathbf{p}^{(r)}} \neq 0$ (see (31) and (33)), equation (34) can be solved for $y^{(r)}$:

$$y^{(r)} = H(x, y, y^{(1)}, \ldots, y^{(r-1)}), \tag{35}$$

where function H is smooth in a neighborhood $\mathbf{p}^{(r)} \in J^r$. From the uniqueness theorem for the solutions of ODE it follows that $f_1(x) = f_3(x)$ on an interval $I \ni x_1$. Since $\mathcal{X}_1$ and $\mathcal{X}_3$ are irreducible algebraic curves it follows that $\mathcal{X}_1 = \mathcal{X}_3$. Therefore, $\mathcal{X}_1 = g \cdot \mathcal{X}_2$.

□

8.3 Proof of Theorem 24.

1. We note that $\dim \mathcal{A}(2) = 6$. We will prove the separation property of $\mathcal{I}_{\mathcal{A}} = \{K_{\mathcal{A}}, T_{\mathcal{A}}\}$ given by (26) on a Zariski open subset

$$W^6 = \{\mathbf{p}^{(6)} \in J^6 \,|\, y^{(2)} \neq 0 \text{ and } 3\, y^{(2)}\, y^{(4)} - 5\,[y^{(3)}]^2 \neq 0\}$$

of J^6 and the separation property of $K_{\mathcal{A}}$ on $W^5 = \pi_5^6(W^6)$. An affine transformation can be written as a product of a Euclidean, an upper triangular area preserving linear transformation, a scaling and a reflection.

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} h & 0 & 0 \\ 0 & h & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} e & f & 0 \\ 0 & \frac{1}{e} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} c & -s & a \\ s & c & b \\ 0 & 0 & 1 \end{pmatrix},$$

where $c^2 + s^2 = 1$, $\epsilon = \pm 1$ and $h \neq 0$.

A Euclidean transformation with

$$c = \frac{1}{\sqrt{1 + [y^{(1)}]^2}}, \quad s = -\frac{y^{(1)}}{\sqrt{1 + [y^{(1)}]^2}}, \quad a = -\frac{y^{(1)}\, y + x}{\sqrt{1 + [y^{(1)}]^2}}, \quad b = \frac{y^{(1)}\, x - y}{\sqrt{1 + [y^{(1)}]^2}}. \tag{36}$$

brings a point $\mathbf{p}^{(5)} = (x, y, y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}, y^{(5)})$ to a point $\mathbf{p}_1^{(5)} = (0, 0, 0, y_1^{(2)}, y_1^{(3)}, y_1^{(4)}, y_1^{(5)})$, where $y_1^{(2)} \neq 0$ if and only if $y^{(2)} \neq 0$. An upper triangular transformation with $e = [y_1^{(2)}]^{1/3}$ and $f = \frac{y_1^{(3)}}{3\,[y^{(2)}]^{5/3}}$ brings the point $\mathbf{p}_1^{(5)}$ to a point $\mathbf{p}_2^{(5)} = (0, 0, 0, 1, 0, y_2^{(4)}, y_2^{(5)})$, where $y_2^{(4)} \neq 0$ if and only if $3\, y^{(2)}\, y^{(4)} - 5\,[y^{(3)}]^2 \neq 0$. A scaling transformation with $h = [y_2^{(4)}]^{\frac{1}{3}}$ brings $\mathbf{p}_2^{(5)}$ to a point $\mathbf{p}_3^{(5)} = (0, 0, 0, 1, 0, 1, y_3^{(5)})$. Finally, if $y_3^{(5)} \leq 0$, we can apply a reflection ($\epsilon = -1$) to bring $\mathbf{p}_3^{(5)}$ to $\mathbf{p}_4^{(5)} = (0, 0, 0, 1, 0, 1, y_4^{(5)})$ with $y_4^{(5)} > 0$.

By the above argument, for any $\mathbf{p}^{(5)}, \mathbf{q}^{(5)} \in W^5$, there exist $A, B \in \mathcal{A}(2)$ such that $\mathbf{p}_1^{(5)} = A \cdot \mathbf{p}^{(5)} = (0, 0, 0, 1, 0, 1, y_1^{(5)})$ and $\mathbf{q}_1^{(5)} = B \cdot \mathbf{q}^{(5)} = (0, 0, 0, 1, 0, 1, y_2^{(5)})$, where $y_1^{(5)} \geq 0$ and $y_2^{(5)} \geq 0$. Then since $K_{\mathcal{A}}$ is invariant:

$$K_{\mathcal{A}}(\mathbf{p}^{(5)}) = K_{\mathcal{A}}(\mathbf{p}_1^{(5)}) = 3\,[y_1^{(5)}]^2 \text{ and } K_{\mathcal{A}}(\mathbf{q}^{(5)}) = K_{\mathcal{A}}(\mathbf{q}_1^{(5)}) = 3\,[y_2^{(5)}]^2.$$

Since $y_1^{(5)} \geq 0$ and $y_2^{(5)} \geq 0$

$$K_{\mathcal{A}}(\mathbf{p}^{(5)}) = K_{\mathcal{A}}(\mathbf{q}^{(5)}) \Longleftrightarrow y_1^{(5)} = y_2^{(5)} \Longleftrightarrow \mathbf{p}_1^{(5)} = \mathbf{q}_1^{(5)} \Longleftrightarrow \mathbf{q}^{(5)} = BA^{-1} \cdot \mathbf{p}^{(5)}.$$

and therefore $K_{\mathcal{A}}$ is separating on W^5.

Similarly, for any $\mathbf{p}^{(6)}, \mathbf{q}^{(6)} \in W^6$, there exist $A, B \in \mathcal{A}(2)$ such that $\mathbf{p}_1^{(5)} = A \cdot \mathbf{p}^{(5)} = (0, 0, 0, 1, 0, 1, y_1^{(5)}, y_1^{(6)})$ and $\mathbf{q}_1^{(6)} = B \cdot \mathbf{q}^{(6)} = (0, 0, 0, 1, 0, 1, y_2^{(5)}, y_2^{(6)})$, where $y_1^{(6)} \geq 0$ and $y_2^{(6)} \geq 0$. Then since $K_{\mathcal{A}}$ and $T_{\mathcal{A}}$ are invariant:

$$\left\{ \begin{array}{lclcl} K_{\mathcal{A}}(\mathbf{p}^{(6)}) & = & K_{\mathcal{A}}(\mathbf{p}_1^{(6)}) & = & 3\,[y_1^{(5)}]^2 \\ T_{\mathcal{A}}(\mathbf{p}^{(6)}) & = & T_{\mathcal{A}}(\mathbf{p}_1^{(6)}) & = & y_1^{(6)} - 5 \end{array} \right. \text{ and } \left\{ \begin{array}{lclcl} K_{\mathcal{A}}(\mathbf{q}^{(6)}) & = & K_{\mathcal{A}}(\mathbf{q}_1^{(6)}) & = & 3\,[y_2^{(5)}]^2 \\ T_{\mathcal{A}}(\mathbf{q}^{(6)}) & = & T_{\mathcal{A}}(\mathbf{q}_1^{(6)}) & = & y_2^{(6)} - 5 \end{array} \right.$$

Then

$$\left\{ \begin{array}{lcl} K_{\mathcal{A}}(\mathbf{p}^{(6)}) & = & K_{\mathcal{A}}(\mathbf{q}^{(6)}) \\ T_{\mathcal{A}}(\mathbf{p}^{(6)}) & = & T_{\mathcal{A}}(\mathbf{q}^{(6)}) \end{array} \right. \Longleftrightarrow \left\{ \begin{array}{lcl} y_1^{(5)} & = & y_2^{(5)} \\ y_1^{(6)} & = & y_2^{(6)} \end{array} \right. \Longleftrightarrow \mathbf{p}_1^{(6)} = \mathbf{q}_1^{(6)} \Longleftrightarrow \mathbf{q}^{(6)} = BA^{-1} \cdot \mathbf{p}^{(6)}.$$

and thus the separation property of $\{K_{\mathcal{A}}, T_{\mathcal{A}}\}$ on J^6 is proved.

2. We note that $\dim \mathcal{PGL}(3) = 8$. We will prove the separation property of $\mathcal{I}_{\mathcal{P}} = \{K_{\mathcal{P}}, T_{\mathcal{P}}\}$ given by (27) on a Zariski open subset

$$W^8 = \{\mathbf{p}^{(8)} \in J^8 \,|\, y^{(2)} \neq 0 \text{ and } 9\, y^{(5)}\, [y^{(2)}]^2 - 45\, y^{(4)}\, y^{(3)}\, y^{(2)} + 40\, [y^{(3)}]^3 \neq 0\}$$

of J^8 and the separation property of $K_{\mathcal{P}}$ on $W^7 = \pi^8_7(W^8)$.

Observe that any element in $A \in \mathcal{PGL}(3)$ can be written as the following product:

$$A = \begin{pmatrix} g & hg & 0 \\ 0 & g^2 & 0 \\ h & i & 1 \end{pmatrix} \begin{pmatrix} e & f & 0 \\ 0 & \frac{1}{e} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} c & -s & a \\ s & c & b \\ 0 & 0 & 1 \end{pmatrix},$$

where $c^2 + s^2 = 1$, $e \neq 0$ and $g \neq 0$. In the first part of the proof, we have shown that the two matrices on the right can bring a point $\mathbf{p}^{(8)} \in W^8$ to the point $\mathbf{p}_1^{(8)} = (0, 0, 0, 1, 0, y_1^{(4)}, \ldots, y_1^{(8)})$. Observe that W^8 is invariant under these transformations. Therefore $\mathbf{p}_1^{(8)} \in W^8$ and hence $y_1^{(5)} \neq 0$. The last transformation with

$$g = [y_1^{(5)}]^{1/3}, h = \frac{1}{3} \frac{5\, [y_1^{(4)}]^2 - y_1^{(6)}}{y_1^{(5)}} \text{ and } i = \frac{1}{18} \frac{[y_1^{(6)}]^2 - 10\, y_1^{(6)}\, [y_1^{(4)}]^2 - 3\, [y_1^{(5)}]^2\, y_1^{(4)} + 25\, [y_1^{(4)}]^4}{[y_1^{(5)}]^2}$$

brings $\mathbf{p}_1^{(8)}$ to $\mathbf{p}_2^{(8)} = (0, 0, 0, 1, 0, 0, 1, 0, y_2^{(7)}, y_2^{(8)})$. A direct computation shows that $K_{\mathcal{P}}(\mathbf{p}_2^{(8)}) = [y_2^{(7)}]^3$ and $T_{\mathcal{P}}(\mathbf{p}_2^{(8)}) = 3\, y_2^{(8)} - \frac{105}{2}$. We observe that $y_2^{(7)}$ and $y_2^{(8)}$ can be uniquely determined from the values of invariants $K_{\mathcal{P}}$ and $T_{\mathcal{P}}$ and therefore we can complete the proof of the separation property of $K_{\mathcal{P}}$ on W^7 and the separation property of $\{K_{\mathcal{P}}, T_{\mathcal{P}}\}$ on W^8 by an argument similar to the one presented in part 1 of the proof.

□

8.4 Proof of Proposition 25.

In the affine case, we note that $j^5_{\mathcal{X}}(\mathbf{p}) \in J^5 \setminus W^5$ and $j^6_{\mathcal{X}}(\mathbf{p}) \in J^6 \setminus W^6$ if an only if $\kappa|_{\mathcal{X}}(\mathbf{p}) = 0$ or $\mu|_{\mathcal{X}}(\mathbf{p}) = 0$. If $\kappa|_{\mathcal{X}}(\mathbf{p}) = 0$ for more than finite number of points on $\mathcal{X}$, then $\mathcal{X}$ is a line, if $\mu|_{\mathcal{X}}(\mathbf{p}) = 0$ for more than finite number of points on $\mathcal{X}$ then it is a parabola (see [12]). From the explicit formulas (26) we see that $\left.\frac{\partial K_{\mathcal{A}}}{\partial y^{(5)}}\right|_{\mathbf{p}^{(5)}} \neq 0$ and $\left.\frac{\partial T_{\mathcal{A}}}{\partial y^{(6)}}\right|_{\mathbf{p}^{(6)}} \neq 0$ for all $\mathbf{p}^{(5)} \in W^5$ and all $\mathbf{p}^{(6)} \in W^6$. Therefore, if an algebraic curve is not a line or a parabola it is $\{\mathcal{K}_{\mathcal{A}}, \mathcal{T}_{\mathcal{A}}\}$-regular. In the projective case, we note that $j^7_{\mathcal{X}}(\mathbf{p}) \in J^7 \setminus W^7$ and $j^8_{\mathcal{X}}(\mathbf{p}) \in J^8 \setminus W^8$ if an only if $\kappa|_{\mathcal{X}}(\mathbf{p}) = 0$ or $\mu_\alpha|_{\mathcal{X}}(\mathbf{p}) = 0$. If $\mu_\alpha|_{\mathcal{X}}(\mathbf{p}) = 0$ for more than finite number of points on $\mathcal{X}$ then $\mathcal{X}$ is a conic (see [12]). From the explicit formulas (27), we see that $\left.\frac{\partial K_{\mathcal{P}}}{\partial y^{(7)}}\right|_{\mathbf{p}^{(7)}} \neq 0$ and $\left.\frac{\partial T_{\mathcal{P}}}{\partial y^{(8)}}\right|_{\mathbf{p}^{(8)}} \neq 0$ for all $\mathbf{p}^{(7)} \in W^7$ and all $\mathbf{p}^{(8)} \in W^8$. Therefore, if an algebraic curve is not a line or a conic it is $\{\mathcal{K}_{\mathcal{P}}, \mathcal{T}_{\mathcal{P}}\}$-regular. □

8.5 Projection algorithm for arbitrary algebraic curves

In this section we no longer assume that algebraic curves $\mathcal{X}$ and $\mathcal{Z}$ have a rational parameterization. We continue to assume that $\mathcal{Z}$ is not a straight line.

Algorithm 35. (Central projections.)

INPUT: An irreducible polynomial $F(x, y)$ whose zero set is an algebraic curve $\mathcal{X}$ and a prime ideal[10] *$H \subset \mathbb{R}[z_1, z_2, z_3]$ defining algebraic curve $\mathcal{Z} \subset \mathbb{R}^3$.*

OUTPUT: The truth of the statement: $\exists [P] \in \mathcal{CP},$ such that $\mathcal{X} = P(\mathcal{Z})$.

STEPS:

1. *if $\mathcal{X}$ is a line or a conic then follow a special procedure (see Appendix 8.6), else*
2. *evaluate $\mathcal{PGL}(3)$-invariants (22) on $\mathcal{X}$, using (15). Obtain two rational functions $K_{\mathcal{P}}|_{\mathcal{X}}$ and $T_{\mathcal{P}}|_{\mathcal{X}}$ of x and y;*
3. *use an elimination algorithm (see Remark 36) to compute an irreducible polynomial $G \in \mathbb{R}[c_1, c_2, c_3, \hat{x}, \hat{y}]$, which for a fixed $c \in \mathbb{R}^3$ defines the curve $\tilde{\mathcal{Z}}_c = \overline{\left\{ \left(\frac{z_1+c_1}{z_3+c_3}, \quad \frac{z_2+c_2}{z_3+c_3} \right) \,\middle|\, (z_1, z_2, z_3) \in \mathcal{Z} \right\}} \subset \mathbb{R}^2.$;*
4. *evaluate $\mathcal{PGL}(3)$-invariants (22) on $\tilde{\mathcal{Z}}_c$,using (15). Obtain two rational functions $K_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}$ and $T_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}$ of c, $\hat{x}$ and $\hat{y}$;*
5. *determine the truth of the statement:*

$$\exists c \in \mathbb{R}^3 \quad \forall (x, y) \in \mathcal{X} \quad \exists (\hat{x}, \hat{y}) \in \mathbb{R}^2 \quad G(c, \hat{x}, \hat{y}) = 0, \quad K_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}(c,\, \hat{x}, \hat{y}) = K_{\mathcal{P}}|_{\mathcal{X}}(x, y) \text{ and } T_{\mathcal{P}}|_{\tilde{\mathcal{Z}}_c}(c,\, \hat{x}, \hat{y}) = T_{\mathcal{P}}|_{\mathcal{X}}(x, y).$$

Remark 36. *To execute Step 3 of Algorithm 35, we define an ideal $\Xi = H + \left\langle \hat{x}\,(z_3 + c_3) - (z_1 + c_1),\ \hat{y}\,(z_3 + c_3) - (z_2 + c_2),\ \delta\,(z_3 + c_3) - 1 \right\rangle \subset \mathbb{R}[c, \hat{x}, \hat{y}, z_1, z_2, z_3, \delta]$. An elimination algorithm can be used to compute the intersection $\hat{\Xi} = \Xi \cap \mathbb{R}[c, \hat{x}, \hat{y}]$. The zero set of $\hat{\Xi}$ is the closure of the image of the rational map ϕ, defined by $\phi(c_1, c_2, c_3, z_1, z_2, z_3) = \left(c_1, c_2, c_3,\ \frac{z_1+c_1}{z_3+c_3},\ \frac{z_2+c_2}{z_3+c_3}\right)$, from the irreducible variety $\phi \colon \mathbb{R}^3 \times \mathcal{Z}$ to $\mathbb{R}^5$, and, therefore, is an irreducible variety. Since the dimension of this variety equals to 4, it is defined by a single irreducible polynomial $G(c, \hat{x}, \hat{y})$.*

Algorithm 37. (Parallel projections.)

INPUT: An irreducible polynomial $F(x, y)$ whose zero set is an algebraic curve $\mathcal{X}$ and a prime idealH $\subset \mathbb{R}[z_1, z_2, z_3]$ defining algebraic curve $\mathcal{Z} \subset \mathbb{R}^3$.

OUTPUT: The truth of the statement: $\exists [P] \in \mathcal{PP},$ such that $\mathcal{X} = P(\mathcal{Z})$.

STEPS:

1. *if $\mathcal{X}$ is a line or a parabola then follow a special procedure (see Appendix 8.6), else*
2. *evaluate $\mathcal{A}(2)$-invariants (20) on $\mathcal{X}$, using (15). Obtain two rational functions $K_{\mathcal{A}}|_{\mathcal{X}}$ and $T_{\mathcal{A}}|_{\mathcal{X}}$ of x and y;*

[10] Generically, H has two generators, although twisted cubic provides a famous counter-example. The question whether or not any algebraic curve in $\mathbb{R}^3$ (or $\mathbb{C}^3$) is a set-theoretic intersection of two algebraic surfaces remains open [15].

3. *use an elimination algorithm to compute an irreducible polynomial* $G \in \mathbb{R}[\hat{x}, \hat{y}]$*, which defines the curve* $\tilde{\mathcal{Z}} = \overline{\left\{(z_2,\, z_3)\ \Big|\ (z_1, z_2, z_3) \in \mathcal{Z}\right\}} \subset \mathbb{R}^2$*;*
4. *evaluate* $\mathcal{A}(2)$*-invariants (20) on* $\tilde{\mathcal{Z}}$ *using (15). Obtain two rational functions* $K_{\mathcal{A}}|_{\tilde{\mathcal{Z}}}$ *and* $T_{\mathcal{A}}|_{\tilde{\mathcal{Z}}}$ *of* $\hat{x}$ *and* $\hat{y}$*;*
5. *determine the truth of the statement:*

   $$\forall (x,y) \in \mathcal{X} \quad \exists (\hat{x}, \hat{y}) \in \mathbb{R}^2\ G(\hat{x}, \hat{y}) = 0,\ K_{\mathcal{A}}|_{\tilde{\mathcal{Z}}}(\hat{x}, \hat{y}) = K_{\mathcal{A}}|_{\mathcal{X}}(x,y) \text{ and } T_{\mathcal{A}}|_{\tilde{\mathcal{Z}}}(\hat{x}, \hat{y}) = T_{\mathcal{A}}|_{\mathcal{X}}(x,y).$$

   If TRUE *exit the procedure, else*
6. *use an elimination algorithm to compute an irreducible polynomial* $G \in \mathbb{R}[b, \hat{x}, \hat{y}]$*, which for a fixed* $b \in \mathbb{R}$ *defines the curve* $\tilde{\mathcal{Z}}_b = \overline{\left\{(\ z_1 + b\, z_2,\ z_3)\ \Big|\ (z_1, z_2, z_3) \in \mathcal{Z}\right\}} \subset \mathbb{R}^2$*;*
7. *evaluate* $\mathcal{A}(2)$*-invariants (20) on* $\tilde{\mathcal{Z}}_b$ *using (15). Obtain two rational functions* $K_{\mathcal{A}}|_{\tilde{\mathcal{Z}}_b}$ *and* $T_{\mathcal{A}}|_{\tilde{\mathcal{Z}}_b}$ *of* b*,* $\hat{x}$ *and* $\hat{y}$*;*
8. *determine the truth of the statement:*

   $$\exists b \in \mathbb{R} \quad \forall (x,y) \in \mathcal{X} \quad \exists (\hat{x}, \hat{y}) \in \mathbb{R}^2 \quad G(b, \hat{x}, \hat{y}) = 0, \quad K_{\mathcal{A}}|_{\tilde{\mathcal{Z}}_b}(b,\, \hat{x}, \hat{y}) = K_{\mathcal{A}}|_{\mathcal{X}}(x,y) \text{ and } T_{\mathcal{A}}|_{\tilde{\mathcal{Z}}_b}(b,\, \hat{x}, \hat{y}) = T_{\mathcal{A}}|_{\mathcal{X}}(x,y).$$

   If TRUE *exit the procedure, else*
9. *use an elimination algorithm to compute an irreducible polynomial* $G \in \mathbb{R}[a_1, a_2, \hat{x}, \hat{y}]$*, which for a fixed* $a \in \mathbb{R}^2$ *defines the curve* $\tilde{\mathcal{Z}}_b = \overline{\left\{(\ z_1 + a_1\, z_3,\ z_2 + a_2\, z_3)\ \Big|\ (z_1, z_2, z_3) \in \mathcal{Z}\right\}} \subset \mathbb{R}^2$*;*
10. *evaluate* $\mathcal{A}(2)$*-invariants (20) on* $\tilde{\mathcal{Z}}_a$ *using (15). Obtain two rational functions* $K_{\mathcal{A}}|_{\tilde{\mathcal{Z}}_a}$ *and* $T_{\mathcal{A}}|_{\tilde{\mathcal{Z}}_a}$ *of* a_1*,* a_2*,* $\hat{x}$ *and* $\hat{y}$*;*
11. *determine the truth of the statement:*

   $$\exists a \in \mathbb{R}^2 \quad \forall (x,y) \in \mathcal{X} \quad \exists (\hat{x}, \hat{y}) \in \mathbb{R}^2 \quad G(a_1, a_2, \hat{x}, \hat{y}) = 0, \quad K_{\mathcal{A}}|_{\tilde{\mathcal{Z}}_a}(a_1, a_2,\, \hat{x}, \hat{y}) = K_{\mathcal{A}}|_{\mathcal{X}}(x,y) \text{ and } T_{\mathcal{A}}|_{\tilde{\mathcal{Z}}_a}(a_1, a_2,\, \hat{x}, \hat{y}) = T_{\mathcal{A}}|_{\mathcal{X}}(x,y).$$

8.6 Algorithms for exceptional curves

We assume here that $\mathcal{Z}$ is a rational curve. The case when $\mathcal{Z}$ is not rational can be treated similarly.

Algorithm 38. (Central projections to lines and conics.)

INPUT: Rational maps $\Gamma(s) = \big(z_1(s), z_2(s), z_3(s)\big)$*,* $s \in \mathbb{R}$ *and* $\gamma(t) = (x(t),\, y(t))$*,* $t \in \mathbb{R}$ *parametrizing algebraic curves* $\mathcal{Z} \subset \mathbb{R}^3$ *and* $\mathcal{X} \subset \mathbb{R}^2$*, such that* $\Delta_2|_{\mathcal{X}}(t) \equiv 0$ *(see (25)).*

OUTPUT: The truth of the statement: $\exists [P] \in \mathcal{CP}$*, such that* $\mathcal{X} = P(\mathcal{Z})$*.*

STEPS:

1. *if* $\ddot{x}\,\dot{y} - \ddot{y}\,\dot{x} \equiv 0$ *and* $(\ddot{\Gamma} \times \dot{\Gamma}) \cdot \dddot{\Gamma} \equiv 0$ *return TRUE and exit;*
2. *if* $\ddot{x}\,\dot{y} - \ddot{y}\,\dot{x} \equiv 0$ *and* $(\ddot{\Gamma} \times \dot{\Gamma}) \cdot \dddot{\Gamma} \neq 0$ *return FALSE and exit;*
3. *for arbitrary* $c_1, c_2, c_3 \in \mathbb{R}$ *define a curve* $\tilde{\mathcal{Z}}_c$ *parametrized by* $\epsilon_c(s) = \left(\frac{z_1(s)+c_1}{z_3(s)+c_3},\ \frac{z_2(s)+c_2}{z_3(s)+c_3}\right)$*;*

4. *evaluate* $\Delta_2|_{\tilde{\mathcal{Z}}_c}$ *using (25). Obtain a rational function* $\Delta_2|_{\tilde{\mathcal{Z}}_c}$ *of* c *and* s.

5. *determine the truth of the statement:* $\exists c \in \mathbb{R}^3 \quad \forall s \in \mathbb{R} \quad \Delta_2|_{\tilde{\mathcal{Z}}_c}(c, s) = 0.$

Remark 39. *The first two steps of the above algorithm rely on the fact that a space curve can be projected to a line if and only if the space curve is coplanar.*

Algorithm 40. (Parallel projections to lines and parabolas.)

INPUT: Rational maps $\Gamma(s) = \big(z_1(s), z_2(s), z_3(s)\big)$, $s \in \mathbb{R}$ *and* $\gamma(t) = (x(t),\, y(t))$, $t \in \mathbb{R}$ *parametrizing algebraic curves* $\mathcal{Z} \subset \mathbb{R}^3$ *and* $\mathcal{X} \subset \mathbb{R}^2$, *such that* $\Delta_1|_{\mathcal{X}}(t) \equiv 0$ *(see (25)).*

OUTPUT: The truth of the statement: $\exists [P] \in \mathcal{CP},$ *such that* $\mathcal{X} = P(\mathcal{Z})$.

STEPS:

1. *if* $\ddot{x}\,\dot{y} - \ddot{y}\,\dot{x} \equiv 0$ *and* $(\ddot{\Gamma} \times \dot{\Gamma}) \cdot \dddot{\Gamma} \equiv 0$ *return TRUE and exit;*

2. *if* $\ddot{x}\,\dot{y} - \ddot{y}\,\dot{x} \equiv 0$ *and* $(\ddot{\Gamma} \times \dot{\Gamma}) \cdot \dddot{\Gamma} \neq 0$ *return FALSE and exit;*
3. *define a curve* $\tilde{\mathcal{Z}}$ *parametrized by* $\alpha(s) = (z_2(s), z_3(s))$;
4. *evaluate* $\Delta_1|_{\tilde{\mathcal{Z}}}$ *using (25). Obtain a rational function* $\Delta_1|_{\tilde{\mathcal{Z}}}$ *of* s;

5. *determine the truth of the statement:* $\forall s \in \mathbb{R} \quad \Delta_1|_{\tilde{\mathcal{Z}}}(s) = 0.$
   If TRUE *exit the procedure, else*
6. *for arbitrary* $b \in \mathbb{R}$, *define a curve* $\tilde{\mathcal{Z}}_b$ *parametrized by* $\beta_b(s) = (z_1(s) + b\, z_2(s),\, z_3(s))$;
7. *evaluate* $\Delta_1|_{\tilde{\mathcal{Z}}_b}$ *using (25). Obtain a rational function* $\Delta_1|_{\tilde{\mathcal{Z}}_b}$ *of* b *and* s;

8. *determine the truth of the statement:* $\exists b \in \mathbb{R} \quad \forall s \in \mathbb{R} \quad \Delta_1|_{\tilde{\mathcal{Z}}_b}(b, s) = 0.$
   If TRUE *exit the procedure, else*
9. *for arbitrary* $a \in \mathbb{R}^2$, *define a curve* $\tilde{\mathcal{Z}}_a$ *parametrized by* $\delta_a(s) = (z_1(s) + a_1\, z_3(s),\, z_2 + a_2\, z_3(s))$;
10. *evaluate* $\Delta_1|_{\tilde{\mathcal{Z}}_a}$ *using (25). Obtain a rational function* $\Delta_1|_{\tilde{\mathcal{Z}}_a}$ *of* a_1, a_2 *and* s;

11. *determine the truth of the statement:* $\exists a \in \mathbb{R}^2 \quad \forall s \in \mathbb{R} \quad \Delta_1|_{\tilde{\mathcal{Z}}_a}(a, s) = 0.$

Acknowledgements: This project was inspired by a discussion with Peter Stiller of paper [2]. We also thank Hoon Hong, Peter Olver and Agnes Szanto for suggestions and support.

References

[1] G. Arnold, P. F. Stiller, and K. Sturtz, *Object-image metrics for generalized weak perspective projection*, Statistics and analysis of shapes, 2006, pp. 253–279.

[2] G. Arnold and P. F. Stiller, *Mathematical aspects of shape analysis for object recognition*, proceedings of IS&T/SPIE joint symposium, 2007, pp. 11p.

[3] M. Boutin, *Numerically invariant signature curves*, Int. J. Computer Vision **40** (2000), 235–248.

[4] J. M. Burdis, *Object-image correspondence under projections.*, Ph.D. Thesis, North Carolina State University, 2010.

[5] E. Calabi, P. J. Olver, C. Shakiban, A. Tannenbaum, and S. Haker, *Differential and numerically invariant signature curves applied to object recognition*, Int. J. Computer Vision **26** (1998), 107–135.

[6] B. F. Caviness and J. R. Johnson (eds.), *Quantifier elimination and cylindrical algebraic decomposition*, Texts and monographs in symbolic computation, 1998.

[7] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Undergraduate Text in Mathematics, Springer-Verlag, New-York, 1997.

[8] O. Faugeras, *Cartan's moving frame method and its application to the geometry and evolution of curves in the Euclidean, affine and projective planes*, Application of Invariance in Computer Vision, J.L Mundy, A. Zisserman, D. Forsyth (eds.) Springer-Verlag Lecture Notes in Computer Science **825** (1994), 11–46.

[9] J. Feldmar, N. Ayache, and F. Betting, *3D-2D projective registration of free-form curves and surfaces*, Proceedings of the fifth international conference on computer vision, ICCV, IEEE Computer Society, 1995, pp. 549 –556.

[10] S. Feng, I. A. Kogan, and H. Krim, *Classification of curves in 2D and 3D via affine integral signature*, Acta Appl. Math. **109** (2010), no. 3, 903–937.

[11] W. Fulton, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[12] H. W. Guggenheimer, *Differential geometry*, McGraw-Hill, New York, 1963.

[13] C. Hann and M. Hickman, *Projective curvature and integral invariants*, Acta applicandae mathematicae **74** (2002), 549 –556.

[14] R. I. Hartley and A. Zisserman, *Multiple view geometry in computer vision*, Second, Cambridge University Press, 2004.

[15] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. MR0463157 (57 #3116)

[16] H. Hong (ed.), *Special issue on computational quantifier elimination*, The Computer Journal, vol. 36 (5), 1993.

[17] M. K. Hu, *Visual pattern recognition by moment invariants*, IRE Trans. Info. Theory **IT-8** (1962), 179–187.

[18] I. A. Kogan, *Two algorithms for a moving frame construction*, Canad. J. Math. **55** (2003), 266–291.

[19] E. Musso and L Nicolodi, *Invariant signature of closed planar curves*, J. Math. Imaging Vision **35** (2009), 68–85.

[20] P. J. Olver, *Joint invariant signatures*, Found. Comp. Math **1** (2001), 3–67.

[21] J. Sato and R. Cipolla, *Affine integral invariants for extracting symmetry axes*, Image and Vision Computing **15** (1997), 627–635.

[22] A. Tarski, *A decision method for elementary algebra and geometry*, second, Univ. of California Press, Berkeley, 1951.

[23] L. Van Gool, T. Moons, E. Pauwels, and A. Oosterlinck, *Semi-differential invariants*, Geometric Invariance in Computer Vision, J.L. Mundy and A. Zisserman (eds), MIT Press (1992), 157–192.